ESTTA Tracking number:

ESTTA498412

Filing date:

10/05/2012

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE TRADEMARK TRIAL AND APPEAL BOARD

Proceeding	91198858
Party	Plaintiff CaseCentral, Inc.
Correspondence Address	WILLIAM J FRIMEL HEFFERNAN SEUBERT & FRENCH LLP 1075 CURTIS STREET MENLO PARK, CA 94025 UNITED STATES bill@hsfllp.com
Submission	Plaintiff's Notice of Reliance
Filer's Name	William J. Frimel
Filer's e-mail	bill@hsfllp.com
Signature	/William J. Frimel/
Date	10/05/2012
Attachments	CaseCentral - Notice of Reliance No. 1.pdf (4 pages)(36959 bytes) Exh 1.pdf (2 pages)(12970 bytes) Exh 2.pdf (3 pages)(61538 bytes) Exh 3.pdf (1 page)(216103 bytes) Exh 4.pdf (2 pages)(337434 bytes) Exh 5.pdf (2 pages)(401011 bytes) Exh 6.pdf (2 pages)(461747 bytes) Exh 7.pdf (2 pages)(224810 bytes) Exh 7.pdf (2 pages)(1571850 bytes) Exh 9.pdf (5 pages)(1571850 bytes) Exh 10.pdf (1 page)(110922 bytes) Exh 11.pdf (2 pages)(459127 bytes) Exh 12.pdf (6 pages)(2456933 bytes) Exh 13.pdf (10 pages)(124278 bytes) Exh 14.pdf (1 page)(5895 bytes) Exh 15.pdf (5 pages)(60042 bytes) Exh 16.pdf (9 pages)(30039 bytes) Exh 17.pdf (4 pages)(1245323 bytes) Exh 19.pdf (3 pages)(544880 bytes) Exh 19.pdf (3 pages)(612672 bytes) Exh 20.pdf (3 pages)(835594 bytes) Exh 21.pdf (5 pages)(844544 bytes) Exh 22.pdf (5 pages)(844544 bytes) Exh 23.pdf (6 pages)(30493 bytes)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE TRADEMARK TRIAL AND APPEAL BOARD

CASECENTRAL, INC.,) Mark: PRESERVATION) CLOUD
	Opposer,) Serial No.: 77/922,469
vs. NEXTPOINT, INC.,) Opposition No. 91198858)
	Applicant.) Published in the Official) Gazette on November 9, 2010

OPPOSER CASECENTRAL, INC.'S NOTICE OF RELIANCE NO. 1

PLEASE TAKE NOTICE THAT, pursuant to (1) the parties' Stipulation to Authenticity of Previously Produced Documents (the "Produced Document Stipulation") (attached as Exhibit 1 hereto), which permits documents previously produced by the parties in the prior litigation between the parties in the United States District Court for the Northern District of Illinois and the above-referenced proceeding to be made of record by way of a Notice of Reliance, without the need for deposition testimony authenticating or referencing such documents, and (2) the parties' Stipulation to Authenticity of Website Printouts (the "Website Stipulation") (attached as Exhibit 2 hereto), which permits certain printouts of websites to be made of record by way of a Notice of Reliance, without the need for deposition testimony authenticating or referencing such documents, Opposer CaseCentral, Inc. ("CaseCentral") offers the following attached exhibits into evidence.

The chart below specifies where an exhibit is submitted pursuant to one of the above-described stipulations.

The exhibits referenced below are submitted on a confidential basis pursuant to the Stipulated Order as to Provisions for Protecting Confidentiality of Information Revealed During Board Proceeding, being filed concurrently herewith.

<u>Exhibit</u>	<u>Description</u>
1	Stipulation to Authenticity of Previously Produced Documents between CaseCentral and Applicant Nextpoint, Inc. ("Nextpoint"), August 20, 2012
2	Stipulation to Authenticity of Website Printouts between CaseCentral and Nextpoint, September 25, 2012
3	Printout of front page of Nextpoint's www.nextpoint.com website, as of September 21, 2012 (submitted pursuant to the Website Stipulation described above)
4	Printout of front page of Nextpoint's www.cloudpreservation.com website, as of September 21, 2012 (submitted pursuant to the Website Stipulation)
5	Printout of front page of the www.networksolutions.com site showing Christopher Kruse's ownership of the www.preservationcloud.com domain name (submitted pursuant to the Website Stipulation)
6	Printout of front page of the www.preservationcloud.com website as of September 21, 2012 (submitted pursuant to the Website Stipulation)
7	Nextpoint press release, dated August 3, 2010 (submitted pursuant to the Produced Document stipulation described above)
8	E-mail from Rakesh Madhava to Michael Beumer and Ben Wolf, dated January 19, 2010 (submitted pursuant to the Produced Document stipulation)
9	Nextpoint's application for the CLOUD PRESERVATION mark, dated April 23, 2010
10	Nextpoint press release, dated June 2, 2010 (submitted pursuant to the Produced Document stipulation)
11	Printout of www.nextpoint.com website (submitted pursuant to the Website Stipulation)

REDACTED PUBLIC VERSION

12	Letters from the United States Patent and Trademark Office to John A. Cullis, Esq., dated October 27, 2010
13	Nextpoint's Responses to CaseCentral's Requests for Admission (Set One), dated December 17, 2010
14	E-mail from Michael Beumer to thelab@nextpoint.com and Rakesh Madhava, dated March 9, 2010 (submitted pursuant to the Produced Document stipulation)
15	Notice of Opposition filed by CaseCentral on March 7, 2011
16	Answer to Notice of Opposition and Affirmative Defenses filed by Nextpoint on April 18, 2011
17	"Archiving and the cloud," <i>The Register</i> , November 1, 2011, available at www.theregister.co.uk/2011/11/01/snia_cloud_archive_best_practices/ (submitted pursuant to the Website Stipulation)
18	"Digital Preservation Cloud Services for Libraries and Archives," Digital Library Foundation, October 31, 2011, available at https://www.diglib.org/forums/2011forum/schedule/digital-preservation-cloud-services-for-libraries-and-archives/ (submitted pursuant to the Website Stipulation)
19	Desire Athow, "Future Evolution of Data Protection Is Data Retention and Preservation Cloud, Says Sepaton CEO," August 7, 2008, available at www.itproportal.com/2008/08/07/ (submitted pursuant to the Website Stipulation)
20	Steve Todd, "Research Papers Moving to the Cloud," November 10, 2009, available at www.stevetodd.typepad.com/my_weblog/2009/11/research-papers-move-to-the-cloud.html (submitted pursuant to the Website Stipulation)
21	Joseph A. Nicholson, "Plus Ultra: Third-Party Preservation in a Cloud Computing Paradigm," <i>Hastings Business Law Journal</i> , October 30, 2011
22	"Digital Library Federation Fall Forum 2011," Dartmouth College Library, November 15, 2011, available at www.dartmouthpreservation.blogspot.com/2011/11/digital-library-federation-fall-forum.html (submitted pursuant to the Website Stipulation)
23	Trademark/Service Mark Application by Nextpoint for the PRESERVATION CLOUD mark, January 28, 2010

REDACTED PUBLIC VERSION

Dated: October 5, 2012

WILLIAM J. FRIMEL

Attorneys for Opposer CASECENTRAL, INC.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE TRADEMARK TRIAL AND APPEAL BOARD

VS. NEXTPOINT, INC.,	Opposer, Applicant.) Mark: PRESERVATION) CLOUD) Serial No.: 77/922,469) Opposition No. 91198858) Published in the Official) Gazette on November 9, 2010)
CERTIFICATE OF SERVICE		
I, Christopher R. Edgar,	, am over the age of e	eighteen and not a party to the above-
referenced action. On October 5, 2012, I served the following document by FedEx		
overnight delivery:		
OPPOSER CASECENTRAL, INC.'S NOTICE OF RELIANCE NO. 1		
I served the foregoing document by FedEx overnight delivery on the counsel		
listed below:		
Daliah Saper, Esq. Saper Law Offices 505 N. Lasalle, Suite 350 Chicago, IL 60654 Attorneys for Applicant Nextpo	oint, Inc.	
I declare under penalty of perjury that the foregoing is true and correct.		

//

//

Dated: October 5, 2012

Christopher R. Edgar

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE TRADEMARK TRIAL AND APPEAL BOARD

CASECENTRAL, INC.,) Mark: PRESERVATION) CLOUD
	Opposer,) Serial No.: 77/922,469
vs. NEXTPOINT, INC.,) Opposition No. 91198858)
	Applicant.) Published in the Official) Gazette on November 9, 2010

STIPULATION TO AUTHENTICITY OF PREVIOUSLY PRODUCED DOCUMENTS

The parties to the above-referenced proceeding (the "TTAB Proceeding") hereby stipulate to the authenticity of the documents previously produced by the parties in (1) the litigation between the parties that took place in the United States District Court for the Northern District of Illinois; and (2) the TTAB Proceeding (collectively, the "Previously Produced Documents"). The parties further stipulate that the Previously Produced Documents may be made of record in the TTAB Proceeding by way of a Notice of Reliance, without the need for deposition testimony authenticating or otherwise referencing the Previously Produced Documents.

The parties make this stipulation without waiving any objection to the admissibility of the Previously Produced Documents.

//

Date: August 16, 2012

/s/ William J. Frimel

William J. Frimel Heffernan Seubert & French LLP 1075 Curtis Street Menlo Park, CA 94025

Telephone: (650) 322-3048 Facsimile: (650) 322-2976

bill@hsfllp.com

Attorneys for Opposer CaseCentral, Inc.

Date: August 20, 2012

/s/ Daliah Saper

Daliah Saper Saper Law Offices 505 N Lasalle Suite 350 Chicago, IL 60654 Telephone: (312) 527-4100

Facsimile: (312) 527-5020

ds@saperlaw.com

Attorneys for Applicant Nextpoint, Inc.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE TRADEMARK TRIAL AND APPEAL BOARD

CASECENTRAL, INC.,) Mark: PRESERVATION) CLOUD
	Opposer,) Serial No.: 77/922,469
vs. NEXTPOINT, INC.,) Opposition No. 91198858
	Applicant.) Published in the Official) Gazette on November 9, 2010

STIPULATION TO AUTHENTICITY OF WEBSITE PRINTOUTS

The parties to the above-referenced proceeding (the "TTAB Proceeding") hereby stipulate to the authenticity of the printouts of websites (the "Website Printouts") attached to Opposer CaseCentral, Inc.'s ("CaseCentral") concurrently filed Notice of Reliance No. 1 and described below:

- 1. Front page of Nextpoint's www.nextpoint.com website, as of September 21, 2012.
- 2. Front page of Nextpoint's www.cloudpreservation.com website, as of September 21, 2012.
- 3. Front page of the www.networksolutions.com/whoissearch/preservationcloud.com site, as of September 25, 2012.
- 4. Front page of the www.preservationcloud.com website, as of September 21, 2012.
- 5. Page from Nextpoint's website, located at www.nextpoint.com/who_bios.html, as of September 25, 2012.

- 6. Article on the internet entitled "Archiving and the cloud," *The Register*, November 1, 2011, available at www.theregister.co.uk/2011/11/01/snia_cloud_archive_best_practices/.
- 7. Article on the internet entitled "Digital Preservation Cloud Services for Libraries and Archives," Digital Library Foundation, October 31, 2011, available at https://www.diglib.org/forums/2011forum/schedule/digital-preservation-cloud-services-for-libraries-and-archives/.
- 8. Article on the internet entitled "Future Evolution of Data Protection Is Data Retention and Preservation Cloud, Says Sepaton CEO," August 7, 2008, available at www.itproportal.com/2008/08/07/.
- 9. Article on the internet entitled "Research Papers Moving to the Cloud," November 10, 2009, available at www.stevetodd.typepad.com/my_weblog/2009/11/research-papers-move-to-the-cloud.html.
- 10. Article on the internet entitled "Digital Library Federation Fall Forum 2011," Dartmouth College Library, November 15, 2011, available at www.dartmouthpreservation.blogspot.com/2011/11/digital-library-federation-fall-forum.html.

The parties further stipulate that the Website Printouts may be made of record in the TTAB Proceeding by way of a Notice of Reliance, without the need for deposition testimony. The parties make this stipulation without waiving any objection to the admissibility of the Website Printouts.

Date: September 25, 2012

/s/ William J. Frimel

William J. Frimel Heffernan Seubert & French LLP 1075 Curtis Street Menlo Park, CA 94025

Telephone: (650) 322-3048 Facsimile: (650) 322-2976

bill@hsfllp.com

Attorneys for Opposer CaseCentral, Inc.

Date: September 25, 2012

/s/ Daliah Saper

Daliah Saper Saper Law Offices 505 N Lasalle Suite 350 Chicago, IL 60654

Telephone: (312) 527-4100 Facsimile: (312) 527-5020

ds@saperlaw.com

Attorneys for Applicant Nextpoint, Inc.



PRESERVATION

DISCOVERY

TRIAL

ABOUT US



Check Out Nextpoint's Weekly Webinar Series to Learn More About Our Products



A Fresh Perspective in Legal Technology

INTEGRATED TECHNOLOGY WITH REAL BENEFITS & LOWER COST

Nextpoint is the leading developer of cloud-based technology products for legal and compliance needs. Our highly secure data cloud integrates applications, processing, storage and support from preservation through resolution. Nextpoint is dedicated to a simple but essential mission: To deliver world-class technology with an uncompromising commitment to engineering, design, and customer service.

learn more>

Trusted by the Best

LEADING CORPORATE & LEGAL CUSTOMERS







verizon









CUSTOMER LOG IN

CONTACT US

1-773-929-4000

NEXTPOINT@TWITTER

NEXTPOINTLAB@TWITTER

NEXTPOINT BLOG: FRANK

PRODUCT BLOG: THE LAB

Privacy Policy / Customer Terms / Customer Support / ©2010 Nextpoint, All Rights Reserved.

1/1 nextpoint.com



The Fully Automated Web Archive Service

Cloud Preservation™ securely archives and indexes data from your WEBSITES, BLOGS, TWITTER and FACEBOOK. It's a fully automated service that sensibly addresses your organization's compliance and regulatory obligations.

- Start automated crawling in minutes
- 100% Web-based no installation necessary
- Archive, search, tag and export data
- Low cost monthly service packages

Try it risk-free for 14 days!

GET STARTED





WHY ARCHIVE?

Most organizations have invested countless resources creating and managing their web presence (websites, blogs, and social media) but few have a consistent way of historically archiving and researching that information.

For most organizations there are very real risks associated with NOT preserving web content. A stringent regulatory environment, greater focus on privacy policies, and evolving electronic data preservation standards have highlighted these risks.



GET COMPLIANT NOW

Maintaining an archive of your online properties and fully understanding **regulatory and compliance concerns** that apply to your industry is essential for any modern organization.

Getting compliant is now made easy with Cloud Preservation. Some industries with more obvious compliance guidelines are:

- Legal
- Government
- Healthcare
- Financial Services



Recent case law clearly outlines an **obligation to maintain active archives of web content** to avoid spoliation.

An immediate, low-cost solution for e-discovery readiness—Cloud Preservation gives you the power to simply and reliably produce historical web data.

Download our informative e-book 10 Steps to Social Media Discovery Readiness to help you get started with a sound strategy for social media discovery.



SIGN UP IN MINUTES!

Preserving your organization's web content is just a few simple steps away. The intake process is easy, secure, and your Cloud
Preservation account will be up and running in no time flat.

It is that simple. Your preserved data will be there when you need it. Log in securely from anywhere, search, tag, and export data quickly and easily.

- Learn More About Pricing >
- Sign Up Now >
- Join Weekly Live Demo >



Cloud Preservation is a Nextpoint Product

4043 N. Ravenswood Avenue | Suite 317 | Chicago, IL 60613

SIGN UP

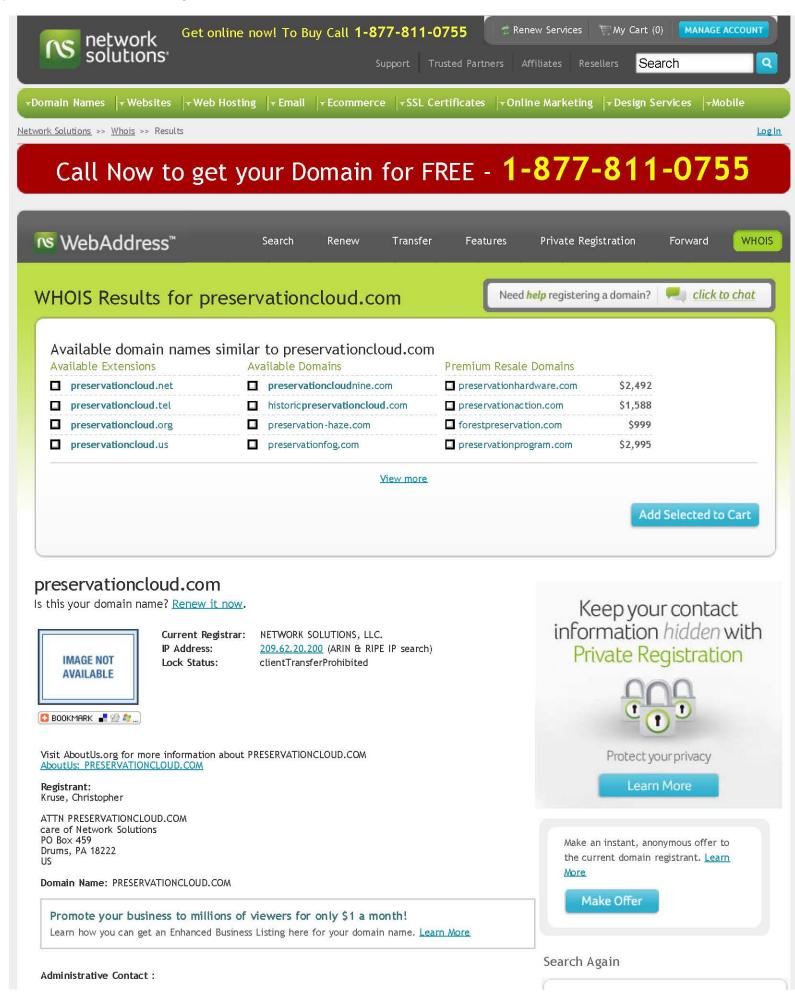
New Customers sign up today to get started with Nextpoint Cloud Preservation!

Secure Log In | Customer Support | Privacy Policy | Customer Terms

nextpoint.com

Copyright Nextpoint, Inc. 2010 All rights reserved.

cloudpreservation.com 2/2



Kruse, Christopher yj 528 72 f8gu@networksolutionsprivateregistration.com ATTN PRESERVATIONCLOUD.COM care of Network Solutions

PO Box 459 Drums, PA 18222 Phone: 570-708-8780

Technical Contact: Kruse, Christopher

yj 528 72 f8gu@networksolutionsprivateregistration.com ATTN PRESERVATIONCLOUD.COM

care of Network Solutions

PO Box 459 Drums, PA 18222

Phone: 570-708-8780

Record expires on 25-Aug-2012 Record created on 25-Aug-2008 Database last updated on 26-Jun-2010

Domain servers in listed order:

NS59. WORLDNIC.COM NS60, WORLDNIC, COM Manage DNS

205, 178, 190, 30 206, 188, 198, 30

This listing is a Network Solutions Private Registration. Mail correspondence to this address must be sent via USPS Express Mail^m or USPS Certified Mail[®], all other mail will not be processed. Be sure to include the registrant's domain name in the address.

Show underlying registry data for this record

Search again here...

Search by either

<u>Domain Name</u> e.g. networksolutions.com <u>IP Address</u> e.g. 205.178, 187, 13

Search



Get online today with our best deals!

Call 1-877-811-0755 for a Network Solutions Sales Expert.



Partner with Network Solutions:

Affiliate Program | Reseller Programs | Refer a Friend

Products

Domain Names Email Hosting Websites Ecommerce Web Hosting SSL Certificates Online Marketing

Design Services

Affiliates & Resellers Affiliate Program UK Affiliate Programme Reseller Program

Support Customer Support Contact Us Customer Feedback Resources WHOIS Search Small Business Blog Small Business Success Labs

Company Information About Us Why Choose Us

Careers News

Promotions & Free Offers

Earn Airline Miles Free Website

Contact Us | Follow Us:

Privacy Policy | Terms of Use | Legal & Policies | Company Info | Site Map | Contact Us Copyright © 2011 Network Solutions, LLC All rights reserved.

Secure Transaction: For your protection, this website is secured with the highest level of SSL Certificate encryption.





PreservationCloud.com

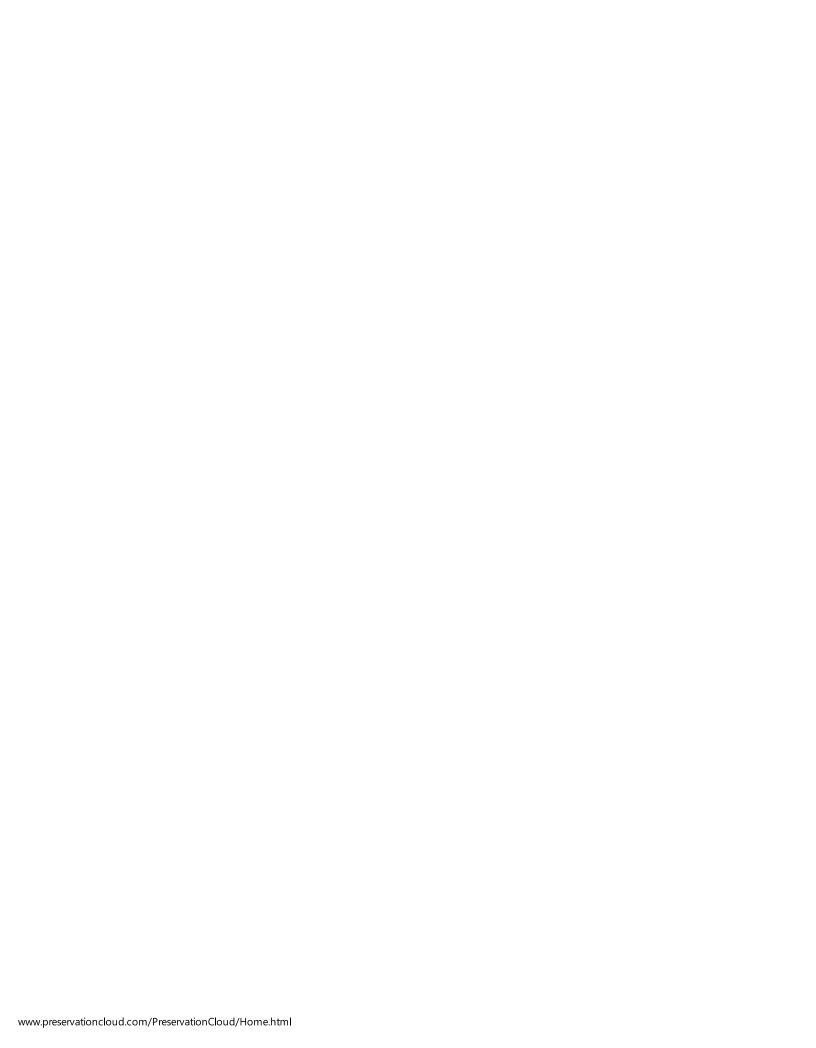
Why not use a secure location on the internet to preserve, store and access ESI collected for legal compliance purposes?

What Is This All About?

Highly touted new technology which preserves your data on a private secure server. This is different from the memory of your individual computer. The private Cloud is a description of a secure server which is located on the internet and is available from anywhere on the web to access data. This sounds like a great way to store data and to expand your storage capacity without the investment in additional hardware. Why not do it??

If this description sounds too good to be true, you should consider both the advantages and disadvantages of storage on the web. For companies with documents which require confidential treatment and for the legal team which provide services to such clients, CaseCentral, Inc. has devised a full range of services thru the use of the CaseCentral eDiscovery Cloud, the on-demand software which permits you to put your data into a server operated by CaseCentral, Inc. as a "Private Cloud". Because the exact location of stored data is known, and access is limited to subscribers authenticated by well know security protocols, the confidentiality of the data is fully protected and available only to fully authenticated sources in satisfaction of the legal ethical requirements of lawyers to protect the confidentially of client data.

If this sounds like it might be a solution for you, please click below and proceed to www.casecentral.com





PRESERVATION

DISCOVERY

TRIAL

ABOUT US

OVERVIEW

SAFE + SOUND

WHO'S USING IT

NEXTPOINT NEWS

CONTACT US

PRESS RELEASE

Nextpoint Announces The Full Launch of Cloud Preservation

Company Releases Automated Archiving Service for Web-based Content

CHICAGO- August 03, 2010

Nextpoint, Inc., the nation's leading provider of cloud-based technology products to law firms and corporate law departments, today announces the full release of Cloud Preservation™, a revolutionary web archiving service that securely captures and indexes data from websites, blogs, Twitter and Facebook feeds.

Cloud Preservation is an immediate, low-cost solution that allows users to schedule crawls that can archive social networking sites, blogs and public-facing websites. The product was originally launched in early June to a select group of beta users who tried the product and provided feedback to the development team at Nextpoint.

With Cloud Preservation, the ability to archive, search, and download web-based data is now available to corporations, law firms, organizations and even individuals answering compliance, regulatory and litigation requirements.

"We are very excited to bring this product to the marketplace," stated Rakesh Madhava, Nextpoint CEO. "We heard from our customers there was a need for a simple archiving solution for their intellectual assets on the web and we are pleased to provide them with the progressive technology and expertise to fill this need."

Madhava added, "We are very thankful for all the users we had for the beta launch of Cloud Preservation. They provided us with valuable feedback and ultimately helped us design the product to fulfill the needs of all users."

More information on Cloud Preservation can be found at www.cloudpreservation.com.

About Nextpoint

Nextpoint (www.nextpoint.com) is a leader in delivering cloud computing products and services to the legal industry. Our world-class, cloud-based platform answers the unique legal, regulatory, and compliance requirements posed by data stored in "the cloud." Trusted by leading corporations and blue-chip law firms, Nextpoint provides a better platform to manage sensitive business-critical information.

Contact:

Elyse Fleischman P: 773.929.4000 E: efleischman@nextpoint.com

CUSTOMER LOG IN

CONTACT US

1-773-929-4000 NEXTPOINT@TWITTER NEXTPOINTLAB@TWITTER NEXTPOINT BLOG: FRANK PRODUCT BLOG: THE LAB

Privacy Policy I Customer Terms I Customer Support I @2010 Nextpoint. All Rights Reserved.

REDACTED - CONFIDENTIAL

Document Description: Application Mail / Create Date: 23-Apr-2010		
Previous Page Next Page	You are currently on page 1 of 2	
PTO Form 1478 (Rev 9/2006) OMB No. 0651-0009 (Exp 12/31/2011)		
 Trademark/Se	rvice Mark Application, Principal Register	

Serial Number: 85021489 Filing Date: 04/23/2010

The table below presents the data as entered.

Input Field	Entered
SERIAL NUMBER	85021489
MARK INFORMATION	
*MARK	\\TICRS\EXPORT10\IMAGEOUT 10\850\214\85021489\xml1\ APP0002.JPG
SPECIAL FORM	YES
USPTO-GENERATED IMAGE	NO
LITERAL ELEMENT	CLOUDPRESERVATION
COLOR MARK	NO
*DESCRIPTION OF THE MARK (and Color Location, if applicable)	The mark consists of an abstract semicircular shape comprised of two intersecting curves, one which represents an abstracted "C" and one and abstracted "P located to the left of the word mark CLOUDPRESERVATION.
PIXEL COUNT ACCEPTABLE	YES
PIXEL COUNT	944 x 325
REGISTER	Principal
APPLICANT INFORMATION	
*OWNER OF MARK	NextPoint Inc.
*STREET	4043 North Ravenswood Ave, Suite 317
*CITY	Chicago
*STATE (Required for U.S. applicants)	Illinois
*COUNTRY	United States

*ZIP/POSTAL CODE (Required for U.S. applicants only)	60613	
LEGAL ENTITY INFORMATION	·	
ТҮРЕ	corporation	
STATE/COUNTRY OF INCORPORATION	Illinois	
GOODS AND/OR SERVICES AND BASIS INFORMATION		
INTERNATIONAL CLASS	042	
*IDENTIFICATION	Providing a web-based software application that permits the archiving, searching and exporting of information and data that is transmitted and displayed on-line	
FILING BASIS	SECTION 1(b)	
ATTORNEY INFORMATION		
NAME	John A Cullis	
ATTORNEY DOCKET NUMBER	17699.08T1	
FIRM NAME	Neal, Gerber & Eisenberg LLP	
INTERNAL ADDRESS	c/o Trademark Administrator	
STREET	2 North LaSalle Street, Suite 1700	
CITY	Chicago	
STATE	Illinois	
COUNTRY	United States	
ZIP/POSTAL CODE	60602	
PHONE	312.269.8000	
FAX	312.269.1747	
EMAIL ADDRESS	trademarks@ngelaw.com	
AUTHORIZED TO COMMUNICATE VIA EMAIL	Yes	
OTHER APPOINTED ATTORNEY	all other attorneys	
CORRESPONDENCE INFORMATION		
NAME	John A Cullis	
FIRM NAME	Neal, Gerber & Eisenberg LLP	
INTERNAL ADDRESS	c/o Trademark Administrator	
STREET	2 North LaSalle Street, Suite 1700	
CITY	Chicago	
STATE	Illinois	

COUNTRY	United States	
ZIP/POSTAL CODE	60602	
PHONE	312.269.8000	
FAX	312.269.1747	
EMAIL ADDRESS	trademarks@ngelaw.com	
AUTHORIZED TO COMMUNICATE VIA EMAIL	Yes	
FEE INFORMATION		
NUMBER OF CLASSES	1	
FEE PER CLASS	325	
*TOTAL FEE DUE	325	
*TOTAL FEE PAID	325	
SIGNATURE INFORMATION		
SIGNATURE	/Rakesh Madhava/	
SIGNATORY'S NAME	Rakesh Madhava	
SIGNATORY'S POSITION	CEO	
DATE SIGNED	04/23/2010	

PTO Form 1478 (Rev 9/2006) OMB No. 0651-0009 (Exp 12/31/2011)

Trademark/Service Mark Application, Principal Register

Serial Number: 85021489 Filing Date: 04/23/2010

To the Commissioner for Trademarks:

MARK: CLOUDPRESERVATION (stylized and/or with design, see mark)

The literal element of the mark consists of CLOUDPRESERVATION.

The applicant is not claiming color as a feature of the mark. The mark consists of an abstract semicircular shape comprised of two intersecting curves, one which represents an abstracted "C" and one and abstracted "P located to the left of the word mark CLOUDPRESERVATION.

The applicant, NextPoint Inc., a corporation of Illinois, having an address of

4043 North Ravenswood Ave, Suite 317

Chicago, Illinois 60613

United States

requests registration of the trademark/service mark identified above in the United States Patent and Trademark Office on the Principal Register established by the Act of July 5, 1946 (15 U.S.C. Section 1051 et seq.), as amended, for the following:

International Class 042: Providing a web-based software application that permits the archiving, searching and exporting of information and data that is transmitted and displayed on-line

Intent to Use: The applicant has a bona fide intention to use or use through the applicant's related company or licensee the mark in commerce on or in connection with the identified goods and/or services. (15 U.S.C. Section 1051(b)).

The applicant's current Attorney Information: John A Cullis and all other attorneys of Neal, Gerber & Eisenberg LLP

c/o Trademark Administrator 2 North LaSalle Street, Suite 1700 Chicago, Illinois 60602 United States

The attorney docket/reference number is 17699.08T1.

The applicant's current Correspondence Information:

John A Cullis
Neal, Gerber & Eisenberg LLP
c/o Trademark Administrator
2 North LaSalle Street, Suite 1700
Chicago, Illinois 60602
312.269.8000(phone)
312.269.1747(fax)

trademarks@ngelaw.com (authorized)

A fee payment in the amount of \$325 has been submitted with the application, representing payment for 1 class(es).

Declaration

The undersigned, being hereby warned that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. Section 1001, and that such willful false statements, and the like, may jeopardize the validity of the application or any resulting registration, declares that he/she is properly authorized to execute this application on behalf of the applicant; he/she believes the applicant to be the owner of the trademark/service mark sought to be registered, or, if the application is being filed under 15 U.S.C. Section 1051(b), he/she believes applicant to be entitled to use such mark in commerce; to the best of his/her knowledge and belief no other person, firm, corporation, or association has the right to use the mark in commerce, either in the identical form thereof or in such near resemblance thereto as to be likely, when used on or in connection with the goods/services of such other person, to cause confusion, or to cause mistake, or to deceive; and that all statements made of his/her own knowledge are true; and that all statements made on information and belief are believed to be true.

Signature: /Rakesh Madhava/ Date Signed: 04/23/2010

Signatory's Name: Rakesh Madhava

Signatory's Position: CEO

RAM Sale Number: 7492

RAM Accounting Date: 04/23/2010

Serial Number: 85021489

Internet Transmission Date: Fri Apr 23 11:02:47 EDT 2010 TEAS Stamp: USPTO/BAS-63.85.229.130-2010042311024716

6608-85021489-46014bdb7526f8fa76ad80dbb9 878fc976-DA-7492-20100423101841601691

TDR Home

This document may be displayed as a PDF file containing images without text. You may view online or save the entire document by clicking on the file download icon in the upper right corner of this page. [required PDF viewer] FAO: Are you seeing only the first page of this PDF document?

If you need help:

- General trademark information: Please e-mail <u>TrademarkAssistanceCenter@uspto.gov</u>, or telephone either 571-272-9250 or 1-800-786-9199.
- Technical help: For instructions on how to use TDR, or help in resolving technical glitches, please e-mail <u>TDR@uspto.gov</u>. If outside of the normal business hours of the USPTO, please e-mail <u>Electronic Business Support</u>, or call 1-800-786-9199.
- Questions about USPTO programs: Please e-mail <u>USPTO Contact Center (UCC)</u>.

Please Note:

- The Mail/Create Date is the date the document was loaded into the database; it is not necessarily the mailing date from which the response period, if any, flows. The mailing date is available in the prosecution history in TARR.
- Some filings made through the Trademark Electronic Application System (TEAS) are not uploaded immediately into TDR. Instead, it may take approximately seven (7) calendar days for the upload. If that amount of time has passed and your filing is still not appearing, please e-mail TDR@uspto.gov.

FOR IMMEDIATE RELEASE

NEXTPOINT ANNOUNCES CLOUD PRESERVATION BETA RELEASE

Company Releases Automated Archiving Service for Web-based Content

CHICAGO- June 2, 2010 – Nextpoint, Inc., the nation's leading provider of cloud-based technology products to law firms and corporate law departments, announces the BETA release of Cloud PreservationTM, a revolutionary web archiving service that securely captures and indexes data from Websites, blogs, Twitter and Facebook feeds.

Cloud Preservation is an immediate, low cost solution that allows users to schedule crawls that can archive social networking sites, blogs and public-facing Websites. For complete information or to sign up as a BETA user, please visit: www.cloudpreservation.com.

Today's stringent regulatory environment, greater focus on privacy policies, and evolving electronic data preservation standards have highlighted the challenge of preserving data generated on the Internet. The ability to archive, search, and download Web-based data is now a necessity for corporations, law firms, organizations and even individuals.

"Our goal with Cloud Preservation is to give users an exciting new level of control over web-based data," says Rakesh Madhava, Nextpoint CEO. "Our customers have been asking for a simple archiving solution for their Web-based content for business continuity, regulatory, legal and archival purposes. Nextpoint Cloud Preservation now fills that need."

About Nextpoint

Nextpoint (<u>www.nextpoint.com</u>) is a leader in delivering cloud computing products and services to the legal industry. Our world-class, cloud-based platform answers the unique legal, regulatory, and compliance requirements posed by data stored in "the cloud". Trusted by leading corporations and bluechip law firms, Nextpoint provides a better platform from which to manage sensitive business-critical information.

Contacts:

Carolyn Depko Edge Legal Marketing P: 732.533.5491

E: cdepko@EdgeLegalMarketing.com

Elyse Fleischman Nextpoint P: 773.929.4000

E: efleischman@nextpoint.com



?

?

?

2

TESTIMONIALS

WHO'S USING IT

CASE STUDIES

BIOGRAPHIES

NEXTPOINT NEWS

Who's Next?: Nextpoint's executive management team is comprised of industry leaders and innovators.

Rakesh Madhava | Chief Executive Officer

In his role as Chief Executive Officer, Rakesh leads a unique team of multimedia designers, computer scientists, and communication experts who help trial teams maximize their trial performance. Rakesh founded Nextpoint in 2001, and today his efforts on developing long term relationships with corporations and law firms, as well as handling the company's marketing, sales and new product development functions. Rakesh was formerly the Chief Creative Officer for the company.

During his career, Rakesh has been retained by a number of Fortune 500 companies including Exxon, Verizon, Morgan Stanley and Astellas Pharmaceutical as well as top tier law firms including McDermott Will & Emery, Winston & Strawn, Kirkland & Ellis, Shearman & Sterling, Kellogg, Huber, Hansen, Todd, Evans & Figel, and Novack & Macey. Notable cases Rakesh has personally supported include U.S. v. Ryan, U.S. v. Razmilovic, et al. (Symbol Technologies), Coleman (Ron Perelman) v. Morgan Stanley, and the Tobacco Fee Arbitrations.

Rakesh has 14 years of experience in legal technology and trial support with specific experience in white collar criminal defense, breach of contract, intellectual property, shareholder suits, tortious interference suits and product liability.

Here's a link to Rakesh's Twitter profile.

S. Courtney Gray | Vice President, Technology

Courtney is Nextpoint's Vice President of Technology and a Partner in the company. She is a thought-leader in the field of trial technology and has specialized in high-exposure, high-profile litigation for over twelve years. Her disciplined approach and first-hand experience with the evolution of software and hardware requirements is the basis of her ability to define Nextpoint's industry-leading technology processes. As the Vice President of Technology, she and the evidence management team are constantly looking for innovative ways to more quickly and efficiently integrate with trial teams to put on the most seamless and persuasive trial presentation possible.

Throughout her career, Courtney has worked on many high-exposure cases for top national firms. These firms include Winston & Strawn, McDermott Will & Emery and Kirkland & Ellis. Notable cases she has supported include U.S. v. Ryan, Coleman (Ron Perelman) v. Morgan Stanley, Verizon v. Vonage, as well as National Tobacco Litigation, National Diet Drug Litigation and National Blood Products Litigation.

Ben Wolf | Vice President, Research & Development

Ben heads Nextpoint's Lab which is focused on next generation technology products supporting lawyers in preparing for trial.

Ben is a recognized leader in delivery of Internet-based technology to the legal industry. The

innovations developed at the Nextpoint Lab under Ben's direction have been reviewed and recognized by leading legal publications and technology-oriented websites. Prior to Nextpoint, Ben led the Research & Development group for Hubbard One, now part of Thompson Reuters. Ben was the Chief Architect for the industry-leading Thomson Elite Business Development product line which has been featured in InfoWeek and is currently used by over 30 percent of the AmLaw 100 firms, including Jones Day, Squire Sanders, Sidley, Loeb & Loeb, DLA, and White & Case.

With over 10 years experience in the legal technology industry, Ben has a proven track record of innovation and holds multiple patents in the legal technology space with others pending. His expertise and areas of research are diverse but are primarily centered around highly secure and scalable webbased applications. Specifically Ben has pioneered the implementation of enterprise cloud computing and virtualization technologies in addition to rich browser based applications leveraging AJAX, mobile technologies, and web-services API's.

His extensive background delivering innovative technologies to corporations and law firms gives Ben an key role in the company's market positioning, product development strategy, and overall commitment to delivering excellence to the marketplace.



Document Description: Offc Action Outgoing

Mail / Create Date: 27-Oct-2010

Previous Page

Next Page

You are currently on page 1

9

To: NextPoint Inc. (<u>ipdocket@ngelaw.com</u>)

Subject: U.S. TRADEMARK APPLICATION NO. 77922478 - DISCOVERY CLOUD - 17699-

05T1

Sent: 10/27/2010 2:34:35 PM

Sent As: ECOM117@USPTO.GOV

Attachments: Attachment - 1

Attachment - 2 Attachment - 3 Attachment - 4 Attachment - 5 Attachment - 6 Attachment - 7

UNITED STATES PATENT AND TRADEMARK OFFICE (USPTO) OFFICE ACTION (OFFICIAL LETTER) ABOUT APPLICANT'S TRADEMARK APPLICATION

APPLICATION SERIAL NO. 77922478

MARK: DISCOVERY CLOUD

77922478

CLICK HERE TO RESPOND TO THIS LETTER:

http://www.uspto.gov/teas/eTEASpageD.htm

CORRESPONDENT ADDRESS:

JOHN A. CULLIS NEAL GERBER & EISENBERG LLP 2 N LASALLE ST STE 1700 CHICAGO, IL 60602

APPLICANT: NextPoint Inc.

CORRESPONDENT'S REFERENCE/DOCKET NO:

17699-05T1

CORRESPONDENT E-MAIL ADDRESS:

ipdocket@ngelaw.com

OFFICE ACTION

STRICT DEADLINE TO RESPOND TO THIS LETTER

TO AVOID ABANDONMENT OF APPLICANT'S TRADEMARK APPLICATION, THE USPTO MUST RECEIVE APPLICANT'S COMPLETE RESPONSE TO THIS LETTER **WITHIN 6 MONTHS** OF THE ISSUE/MAILING DATE BELOW.

ISSUE/MAILING DATE: 10/27/2010

Upon further review, the examining attorney has determined the following:

SECTION 2(e)(1) REFUSAL - MERELY DESCRIPTIVE - CLASS 42 ONLY

Registration is refused because the applied-for mark merely describes a function or purpose of applicant's goods and/or services. Trademark Act Section 2(e)(1), 15 U.S.C. §1052(e)(1); see TMEP §§1209.01(b), 1209.03 et seq.

A mark is merely descriptive if it describes an ingredient, quality, characteristic, function, feature, purpose or use of the specified goods and/or services. TMEP §1209.01(b); see In re Steelbuilding.com, 415 F.3d 1293, 1297, 75 USPQ2d 1420, 1421 (Fed. Cir. 2005); In re Gyulay, 820 F.2d 1216, 1217-18, 3 USPQ2d 1009, 1010 (Fed. Cir. 1987).

Generally, a mark that merely combines descriptive words is not registrable if the individual components retain their descriptive meaning in relation to the goods and/or services and the combination results in a composite mark that is itself descriptive. TMEP §1209.03(d); see, e.g., In re King Koil Licensing Co. Inc., 79 USPQ2d 1048, 1052 (TTAB 2006) (holding THE BREATHABLE MATTRESS merely descriptive of beds, mattresses, box springs and pillows where the evidence showed that the term "BREATHABLE" retained its ordinary dictionary meaning when combined with the term "MATTRESS" and the resulting combination was used in the relevant industry in a descriptive sense); In re Associated Theatre Clubs Co., 9 USPQ2d 1660, 1663 (TTAB 1988) (holding GROUP SALES BOX OFFICE merely descriptive of theater ticket sales services because such wording "is nothing more than a combination of the two common descriptive terms most applicable to applicant's services which in combination achieve no different status but remain a common descriptive compound expression").

Only where the combination of descriptive terms creates a unitary mark with a unique, incongruous, or otherwise nondescriptive meaning in relation to the goods and/or services is the combined mark registrable. *See, e.g.*, *In re Colonial Stores*, *Inc.*, 394 F.2d 549, 551, 157 USPQ 382, 384 (C.C.P.A. 1968).

In this case, both the individual components and the composite result are descriptive of applicant's goods and/or services and do not create a unique, incongruous or nondescriptive meaning in relation to the goods and/or services. Specifically, the computer software or cloud will be used in connection with the discovery portion of litigation work. Please see the attached dictionary definitions from Encarta® World English Dictionary [North American Edition] © & (P)2009 Microsoft Corporation, and the identification of services.

Please also see the attached web page evidence from applicant's website www.nextpoint.com which demonstrates that "Nextpoint Discovery Cloud empowers law firms to securely perform native file processing, document review and production with no local software or per-user fees. We optimize cost and time savings and give your legal team the control to review your document set with the utmost speed and ease."

Therefore, the mark is refused under Section 2(e)(1) of the Trademark Act.

Although applicant's mark has been refused registration, applicant may respond to the refusal(s) by submitting evidence and arguments in support of registration.

SUPPLEMENTAL REGISTER

A mark in an application under Trademark Act Section 1(b) is not eligible for registration on the Supplemental Register until an acceptable amendment to allege use under 37 C.F.R. §2.76 has been filed. 37 C.F.R. §82.47(d), 2.75(b); TMEP §§815.02, 1102.03. When a Section 1(b) application is successfully amended to the Supplemental Register, the effective filing date of the application will be the date on which applicant met the minimum filing requirements of 37 C.F.R. §2.76(e) for the amendment to allege use. 37 C.F.R. §2.75(b); TMEP §§816.02, 1102.03.

/Anne Gustason/ Trademark Examining Attorney U.S. Patent and Trademark Office Law Office 117 (571) 272-9722 TO RESPOND TO THIS LETTER: Use the Trademark Electronic Application System (TEAS) response form at http://teasroa.uspto.gov/roa/. Please wait 48-72 hours from the issue/mailing date before using TEAS, to allow for necessary system updates of the application. For technical assistance with online forms, e-mail TEAS@uspto.gov.

WHO MUST SIGN THE RESPONSE: It must be personally signed by an individual applicant or someone with legal authority to bind an applicant (i.e., a corporate officer, a general partner, all joint applicants). If an applicant is represented by an attorney, the attorney must sign the response.

PERIODICALLY CHECK THE STATUS OF THE APPLICATION: To ensure that applicant does not miss crucial deadlines or official notices, check the status of the application every three to four months using Trademark Applications and Registrations Retrieval (TARR) at http://tarr.uspto.gov/. Please keep a copy of the complete TARR screen. If TARR shows no change for more than six months, call 1-800-786-9199. For more information on checking status, see http://www.uspto.gov/trademarks/process/status/.

TO UPDATE CORRESPONDENCE/E-MAIL ADDRESS: Use the TEAS form at http://www.uspto.gov/teas/eTEASpageE.htm.

TDR Home

This document may be displayed as a PDF file containing images without text. You may view online or save the entire document by clicking on the file download icon in the upper right corner of this page. [required PDF viewer] FAQ: Are you seeing only the first page of this PDF document?

If you need help:

- General trademark information: Please e-mail <u>TrademarkAssistanceCenter@uspto.gov</u>, or telephone either 571-272-9250 or 1-800-786-9199.
- Technical help: For instructions on how to use TDR, or help in resolving technical glitches, please e-mail <u>TDR@uspto.gov</u>. If outside of the normal business hours of the USPTO, please e-mail <u>Electronic Business Support</u>, or call 1-800-786-9199.
- Questions about USPTO programs: Please e-mail <u>USPTO Contact Center (UCC)</u>.

Please Note:

- The Mail/Create Date is the date the document was loaded into the database; it is not necessarily the mailing date from which the response period, if any, flows. The mailing date is available in the prosecution history in TARR.
- Some filings made through the Trademark Electronic Application System (TEAS) are not uploaded immediately into TDR. Instead, it may take approximately seven (7) calendar days for the upload. If that amount of time has passed and your filing is still not appearing, please e-mail TDR@uspto.gov.

Document Description: Offic Action Outgoing

Mail / Create Date: 27-Oct-2010

You are currently on page 1

To:

NextPoint Inc. (<u>ipdocket@ngelaw.com</u>)

Subject:

U.S. TRADEMARK APPLICATION NO. 77922489 - TRIAL CLOUD - 17699-06T1

Sent:

10/27/2010 2:35:16 PM

Sent As:

ECOM117@USPTO.GOV

Attachments: Attachment - 1

Attachment - 2

Attachment - 3

Attachment - 4

Attachment - 5

Attachment - 6

Attachment - 7

Attachment - 8

UNITED STATES PATENT AND TRADEMARK OFFICE (USPTO) OFFICE ACTION (OFFICIAL LETTER) ABOUT APPLICANT'S TRADEMARK APPLICATION

APPLICATION SERIAL NO.

77922489

MARK: TRIAL CLOUD

77922489

CORRESPONDENT ADDRESS:

JOHN A. CULLIS

NEAL GERBER & EISENBERG LLP

2 N LASALLE ST STE 1700

CHICAGO, IL 60602

CLICK HERE TO RESPOND TO THIS LETTER:

http://www.uspto.gov/teas/eTEASpageD.htm

APPLICANT:

NextPoint Inc.

CORRESPONDENT'S REFERENCE/DOCKET NO:

17699-06T1

CORRESPONDENT E-MAIL ADDRESS:

ipdocket@ngelaw.com

OFFICE ACTION

STRICT DEADLINE TO RESPOND TO THIS LETTER

TO AVOID ABANDONMENT OF APPLICANT'S TRADEMARK APPLICATION. THE USPTO MUST RECEIVE APPLICANT'S COMPLETE RESPONSE TO THIS LETTER WITHIN 6 MONTHS OF THE ISSUE/MAILING DATE BELOW.

ISSUE/MAILING DATE: 10/27/2010

Upon further review, the examining attorney has determined the following:

SECTION 2(e)(1) REFUSAL – MERELY DESCRIPTIVE – CLASS 42 ONLY

Registration is refused because the applied-for mark merely describes a function or purpose of applicant's goods and/or services. Trademark Act Section 2(e)(1), 15 U.S.C. §1052(e)(1); see TMEP §§1209.01(b), 1209.03 et seq.

A mark is merely descriptive if it describes an ingredient, quality, characteristic, function, feature, purpose or use of the specified goods and/or services. TMEP §1209.01(b); see In re Steelbuilding.com, 415 F.3d 1293, 1297, 75 USPQ2d 1420, 1421 (Fed. Cir. 2005); In re Gyulay, 820 F.2d 1216, 1217-18, 3 USPQ2d 1009, 1010 (Fed. Cir. 1987).

Generally, a mark that merely combines descriptive words is not registrable if the individual components retain their descriptive meaning in relation to the goods and/or services and the combination results in a composite mark that is itself descriptive. TMEP §1209.03(d); see, e.g., In re King Koil Licensing Co. Inc., 79 USPQ2d 1048, 1052 (TTAB 2006) (holding THE BREATHABLE MATTRESS merely descriptive of beds, mattresses, box springs and pillows where the evidence showed that the term "BREATHABLE" retained its ordinary dictionary meaning when combined with the term "MATTRESS" and the resulting combination was used in the relevant industry in a descriptive sense); In re Associated Theatre Clubs Co., 9 USPQ2d 1660, 1663 (TTAB 1988) (holding GROUP SALES BOX OFFICE merely descriptive of theater ticket sales services because such wording "is nothing more than a combination of the two common descriptive terms most applicable to applicant's services which in combination achieve no different status but remain a common descriptive compound expression").

Only where the combination of descriptive terms creates a unitary mark with a unique, incongruous, or otherwise nondescriptive meaning in relation to the goods and/or services is the combined mark registrable. *See, e.g.*, *In re Colonial Stores*, *Inc.*, 394 F.2d 549, 551, 157 USPQ 382, 384 (C.C.P.A. 1968).

In this case, both the individual components and the composite result are descriptive of applicant's goods and/or services and do not create a unique, incongruous or nondescriptive meaning in relation to the goods and/or services. Specifically, the computer software or cloud will be used in connection with civil litigation, or trial, work. Please see the attached dictionary definitions from Encarta® World English Dictionary [North American Edition] © & (P)2009 Microsoft Corporation, and the identification of services.

Please also see the attached web page evidence from applicant's website www.nextpoint.com which demonstrates that "Nextpoint's Trial CloudTM is an effective, cost-efficient platform for managing large volumes of evidence for civil litigation—including depositions, transcripts, e-mail and other electronically stored information (ESI)—in an single, integrated environment. Nextpoint leverages cloud computing technology to elegantly address the challenges of managing large quantities of evidence. For the user, this means even though it's simple to use, it is powerful, infinitely scalable, and accessible from anywhere."

Therefore, the mark is refused under Section 2(e)(1) of the Trademark Act.

Although applicant's mark has been refused registration, applicant may respond to the refusal(s) by submitting evidence and arguments in support of registration.

SUPPLEMENTAL REGISTER

A mark in an application under Trademark Act Section 1(b) is not eligible for registration on the Supplemental Register until an acceptable amendment to allege use under 37 C.F.R. §2.76 has been filed. 37 C.F.R. §82.47(d), 2.75(b); TMEP §§815.02, 1102.03. When a Section 1(b) application is successfully amended to the Supplemental Register, the effective filing date of the application will be the date on which applicant met the minimum filing requirements of 37 C.F.R. §2.76(e) for the amendment to allege use. 37 C.F.R. §2.75(b); TMEP §§816.02, 1102.03.

/Anne Gustason/ Trademark Examining Attorney U.S. Patent and Trademark Office Law Office 117 (571) 272-9722 TO RESPOND TO THIS LETTER: Use the Trademark Electronic Application System (TEAS) response form at http://teasroa.uspto.gov/roa/. Please wait 48-72 hours from the issue/mailing date before using TEAS, to allow for necessary system updates of the application. For technical assistance with online forms, e-mail TEAS@uspto.gov.

WHO MUST SIGN THE RESPONSE: It must be personally signed by an individual applicant or someone with legal authority to bind an applicant (i.e., a corporate officer, a general partner, all joint applicants). If an applicant is represented by an attorney, the attorney must sign the response.

PERIODICALLY CHECK THE STATUS OF THE APPLICATION: To ensure that applicant does not miss crucial deadlines or official notices, check the status of the application every three to four months using Trademark Applications and Registrations Retrieval (TARR) at http://tarr.uspto.gov/. Please keep a copy of the complete TARR screen. If TARR shows no change for more than six months, call 1-800-786-9199. For more information on checking status, see http://www.uspto.gov/trademarks/process/status/.

TO UPDATE CORRESPONDENCE/E-MAIL ADDRESS: Use the TEAS form at http://www.uspto.gov/teas/eTEASpageE.htm.

TDR Home

This document may be displayed as a PDF file containing images without text. You may view online or save the entire document by clicking on the file download icon in the upper right corner of this page. [required PDF viewer] FAQ: Are you seeing only the first page of this PDF document?

If you need help:

- General trademark information: Please e-mail <u>TrademarkAssistanceCenter@uspto.gov</u>, or telephone either 571-272-9250 or 1-800-786-9199.
- Technical help: For instructions on how to use TDR, or help in resolving technical glitches, please e-mail TDR@uspto.gov. If outside of the normal business hours of the USPTO, please e-mail Electronic Business Support, or call 1-800-786-9199.
- Questions about USPTO programs: Please e-mail <u>USPTO Contact Center (UCC)</u>.

Please Note:

- The Mail/Create Date is the date the document was loaded into the database; it is not necessarily the mailing date from which the response period, if any, flows. The mailing date is available in the prosecution history in TARR.
- Some filings made through the Trademark Electronic Application System (TEAS) are not uploaded immediately into TDR. Instead, it may take approximately seven (7) calendar days for the upload. If that amount of time has passed and your filing is still not appearing, please e-mail TDR@uspto.gov.

UNITED STATES DISTRICT COURT NORTHERN DISTRICT OF ILLINOIS EASTERN DIVISION

NEXTPOINT, INC.,)
Plaintiff,)
v.) Case No. 10-cv-03515
CASE CENTRAL, INC.,) Judge Gary Feinerman
Defendant.) Magistrate Judge Jeffrey T. Gilbert

RESPONSE TO DEFENDANT'S REQUESTS FOR ADMISSION (SET ONE)

Plaintiff Nextpoint, Inc. ("Plaintiff" or "Nextpoint"), by its attorneys, Novack and Macey LLP, as and for its Response to Defendant's Requests for Admission to Plaintiff (Set One) (the "Requests") served by Case Central, Inc.'s ("Defendant" or "CaseCentral") states as follows.

GENERAL OBJECTIONS

- A. Plaintiff objects to the Requests to the extent that they purport to impose duties and/or obligations in excess of, or inconsistent with, those imposed by the Federal Rules of Civil Procedure or the local rules or standing orders of this Court.
- B. Plaintiff objects to the Requests to the extent that they call for the disclosure of information that is protected by the attorney-client privilege, the attorney work-product doctrine, any other applicable privilege, or otherwise protected from disclosure.
- C. By responding to the Requests, Plaintiff does not admit the relevancy or admissibility of any fact, or waive any objection based thereon.
- D. Plaintiff's investigation is ongoing. Plaintiff reserves the right to supplement and/or amend its responses at any appropriate time. The responses set forth below are based on the facts currently known to Plaintiff.

RESPONSES

Each specific response incorporates, and is subject to, the General Objections set forth above, which are not waived.

REQUEST FOR ADMISSION NO. 1:

Admit that the Nextpoint Marks are not inherently distinctive.

RESPONSE:

Plaintiff denies this Request.

REQUEST FOR ADMISSION NO. 2:

Admit that the Nextpoint Marks have not acquired secondary meaning.

RESPONSE:

Plaintiff denies this Request.

REQUEST FOR ADMISSION NO. 3:

Admit that CaseCentral's use of the mark "CASECENTRAL EDISCOVERY CLOUD" is not likely to cause consumer confusion as to the source of CaseCentral's products or services.

RESPONSE:

Plaintiff denies this Request.

REQUEST FOR ADMISSION NO. 4:

Admit that the terms "SaaS," "ASP," and "Cloud Computing" have materially the same meaning.

RESPONSE:

Plaintiff denies this Request.

REQUEST FOR ADMISSION NO. 5:

Admit that Nextpoint caused Lisa Peters-Beumer to e-mail CaseCentral in February 2010, seeking to obtain CaseCentral's www.preservationcloud.com domain name.

RESPONSE:

Plaintiff admits an e-mail was sent from Lisa Peters-Beumer's account to Defendant in February 2010 expressing interest in obtaining this www.preservationcloud.com domain name. Plaintiff denies the remainder of this Request.

REQUEST FOR ADMISSION NO. 6:

Admit that Nextpoint was aware, before Nextpoint applied to register the Nextpoint Marks with the United States Patent and Trademark Office, that CaseCentral had registered the www.preservationcloud.com domain name.

RESPONSE:

Plaintiff denies this Request.

REQUEST FOR ADMISSION NO. 7:

Admit that CaseCentral developed and deployed a SaaS application for use in connection with litigation and trial support services before Nextpoint did so.

RESPONSE:

Plaintiff objects to this Request on the grounds that it does not comply with Fed. R. Civ. P. 36(a)(2) in that, among other things, the Request is compound and fails to separately state each matter as to which an admission is sought. Further, the Request is vague and unclear in that, at this time, Plaintiff is not aware of the purported "SaaS application" to which Defendant is referring. With respect to this unidentified, purported application, Defendant has not stated who developed it, who deployed it, when it was developed or when it was deployed.

REQUEST FOR ADMISSION NO. 8:

Admit that CaseCentral developed and deployed an ASP application for use in connection with litigation and trial support services before Nextpoint did so.

RESPONSE:

Plaintiff objects to this Request on the grounds that it does not comply with Fed. R. Civ. P. 36(a)(2) in that, among other things, the Request is compound and fails to separately state each matter as to which an admission is sought. Further, the Request is vague and ambiguous in that, at this time, Plaintiff is not aware of the purported "ASP application" to which Defendant is referring. With respect to this unidentified, purported application, Defendant has not stated who developed it, who deployed it, when it was developed or when it was deployed.

REQUEST FOR ADMISSION NO. 9:

Admit that Nextpoint has no evidence that consumers have actually confused the products and services offered by CaseCentral with those of Nextpoint.

RESPONSE:

Plaintiff denies this Request.

REQUEST FOR ADMISSION NO. 10:

Admit that Nextpoint has not performed or commissioned any studies, surveys or other investigations reflecting that consumers have actually confused the products and services offered by CaseCentral with those offered by Nextpoint.

RESPONSE:

Limiting its response to the time period ending as of the filing of this response, Plaintiff admits this Request.

REQUEST FOR ADMISSION NO. 11:

Admit that Nextpoint makes no claim to the exclusive right to use the word "cloud," separate or apart from the phrases "Discovery Cloud," "Trial Cloud," or "Preservation Cloud."

RESPONSE:

Plaintiff admits this Request.

REQUEST FOR ADMISSION NO. 12:

Admit that the word "cloud," as used in the context of Cloud Computing or the use of computers, has obtained a generic meaning.

RESPONSE:

Plaintiff objects to this Request on the grounds that it does not comply with Fed. R. Civ. P. 36(a)(2) in that, among other things, the Request is compound and fails to separately state each matter as to which an admission is sought. Further, the phrases "Cloud Computing" (which is capitalized) and "the use of computers" are vague, ambiguous and, as to "Cloud Computing," undefined by Defendant. For the foregoing reasons, Plaintiff states that it cannot truthfully admit or deny the request.

REQUEST FOR ADMISSION NO. 13:

Admit that CaseCentral began using the word "cloud" to describe its products and/or services before November 17, 2009.

RESPONSE:

Plaintiff objects to this Request on the grounds that it does not comply with Fed. R. Civ. P. 36(a)(2) in that, among other things, the Request is compound and fails to separately state each matter as to which an admission is sought. Further, Defendant has failed to identify when it allegedly began using the word "cloud," what specific "products and/or services" it was allegedly referring to, who allegedly used the word "cloud" in the manner alleged, and whether the word was used orally or in print -- thereby giving Plaintiff no ability to make a determination regarding the accuracy of Defendant's allegation. For the foregoing reasons, Plaintiff states that it cannot truthfully admit or deny this Request.

REQUEST FOR ADMISSION NO. 14:

Admit that Applied Discovery uses the word "cloud," and/or the phrase "cloud computing," to describe its products and/or services.

RESPONSE:

Plaintiff objects to this Request on the grounds that it does not comply with Fed. R. Civ. P. 36(a)(2) in that, among other things, the Request is compound and fails to separately state each matter as to which an admission is sought. Further, the Request is vague and ambiguous in that Defendant has failed to specify when the referenced entity allegedly used the "the word 'cloud,' and/or the phrase 'cloud computing,'" or what "products and/or services" to which the referenced entity was referring. In addition, Defendant has not specified who made the alleged statements, when they were made, and whether they were made orally or in print. For the foregoing reasons, Plaintiff states that it cannot truthfully admit or deny the request.

REQUEST FOR ADMISSION NO. 15:

Admit that IPRO Tech uses the word "cloud," and/or the phrase "cloud computing," to describe its products and/or services.

RESPONSE:

Plaintiff objects to this Request on the grounds that it does not comply with Fed. R. Civ. P. 36(a)(2) in that, among other things, the Request is compound and fails to separately state each matter as to which an admission is sought. Further, the Request is vague and ambiguous in that Defendant has failed to specify when the referenced entity allegedly used the "the word 'cloud,' and/or the phrase 'cloud computing," or what "products and/or services" to which the referenced entity was referring. In addition, Defendant has not specified who made the alleged statements, when they were made, and whether they were made orally or in print. Subject to the foregoing objections, the General Objections and the subsequent determination of the sufficiency

of such objections pursuant to Fed. R. Civ. P. 36(a)(6), Plaintiff states that it cannot truthfully admit or deny this Request.

REQUEST FOR ADMISSION NO. 16:

Admit that BCPI uses the word "cloud," and/or the phrase "cloud computing," to describe its products and/or services.

RESPONSE:

Plaintiff objects to this Request on the grounds that it does not comply with Fed. R. Civ. P. 36(a)(2) in that, among other things, the Request is compound and fails to separately state each matter as to which an admission is sought. Further, the Request is vague and ambiguous in that Defendant has failed to specify when the referenced entity allegedly used the "the word 'cloud,' and/or the phrase 'cloud computing,'" or what "products and/or services" to which the referenced entity was referring. In addition, Defendant has not specified who made the alleged statements, when they were made, and whether they were made orally or in print. Subject to the foregoing objections, the General Objections and the subsequent determination of the sufficiency of such objections pursuant to Fed. R. Civ. P. 36(a)(6), Plaintiff states that it cannot truthfully admit or deny this Request.

REQUEST FOR ADMISSION NO. 17:

Admit that Clearwell Systems uses the word "cloud," and/or the phrase "cloud computing," to describe its products and/or services.

RESPONSE:

Plaintiff objects to this Request on the grounds that it does not comply with Fed. R. Civ. P. 36(a)(2) in that, among other things, the Request is compound and fails to separately state each matter as to which an admission is sought. Further, the Request is vague and ambiguous in that Defendant has failed to specify when the referenced entity allegedly used the "the word

'cloud,' and/or the phrase 'cloud computing,'" or what "products and/or services" to which the referenced entity was referring. In addition, Defendant has not specified who made the alleged statements, when they were made, and whether they were made orally or in print. Subject to the foregoing objections, the General Objections and the subsequent determination of the sufficiency of such objections pursuant to Fed. R. Civ. P. 36(a)(6), Plaintiff states that it cannot truthfully admit or deny this Request.

REQUEST FOR ADMISSION NO. 18:

Admit that Kroll Ontrack uses the word "cloud," and/or the phrase "cloud computing," to describe its products and/or services.

RESPONSE:

Plaintiff objects to this Request on the grounds that it does not comply with Fed. R. Civ. P. 36(a)(2) in that, among other things, the Request is compound and fails to separately state each matter as to which an admission is sought. Further, the Request is vague and ambiguous in that Defendant has failed to specify when the referenced entity allegedly used the "the word 'cloud,' and/or the phrase 'cloud computing,'" or what "products and/or services" to which the referenced entity was referring. In addition, Defendant has not specified who made the alleged statements, when they were made, and whether they were made orally or in print. Subject to the foregoing objections, the General Objections and the subsequent determination of the sufficiency of such objections pursuant to Fed. R. Civ. P. 36(a)(6), Plaintiff states that it cannot truthfully admit or deny this Request.

REQUEST FOR ADMISSION NO. 19:

Admit that Iron Mountain uses the word "cloud," and/or the phrase "cloud computing," to describe its products and/or services.

RESPONSE:

Plaintiff objects to this Request on the grounds that it does not comply with Fed. R. Civ. P. 36(a)(2) in that, among other things, the Request is compound and fails to separately state each matter as to which an admission is sought. Further, the Request is vague and ambiguous in that Defendant has failed to specify when the referenced entity allegedly used the "the word 'cloud,' and/or the phrase 'cloud computing,'" or what "products and/or services" to which the referenced entity was referring. In addition, Defendant has not specified who made the alleged statements, when they were made, and whether they were made orally or in print. Subject to the foregoing objections, the General Objections and the subsequent determination of the sufficiency of such objections pursuant to Fed. R. Civ. P. 36(a)(6), Plaintiff states that it cannot truthfully admit or deny this Request.

NEXTPOINT, INC.

By:

One of Its Attorneys

Eric N. Macey Richard L. Miller II NOVACK AND MACEY LLP 100 North Riverside Plaza Chicago, IL 60606 (312) 419-6900 Doc. #391988

CERTIFICATE OF SERVICE

Richard L. Miller II, an attorney, hereby certifies that he served the foregoing **Response To Defendant's Requests For Admission (Set One)** by causing a true and correct copy thereof to be delivered by email and U.S. Mail to:

William Frimel
HEFFERMAN, SEUBERT & FRENCH LLP
1075 Curtis Street
Menlo Park, CA 94025
(650) 322-3048
bill@hsfllp.com

Patrick J. Lamb
Reeghan Raffals
VALOREM LAW GROUP
35 East Wacker Drive, Suite 3000
Chicago, IL 60601
(312) 676-5462
patrick.lamb@valoremlaw.com
reeghan.raffals@valoremlaw.com

Christopher R. Edgar 308 Hans Avenue Mountain View, CA 94040 (650) 269-8566 cedgar@stanfordalumni.org

on this 17th day of December 2010.

Richard L. Miller II

REDACTED - CONFIDENTIAL

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE TRADEMARK TRIAL AND APPEAL BOARD

CASECENTRAL, INC.,	Opposer,)) Mark: PRESERVATION) CLOUD)
VS.) Serial No.: 77/922,469
NEXTPOINT, INC.,) Opposition No
	Applicant.) Published in the Official) Gazette on November 9, 2010

NOTICE OF OPPOSITION

CaseCentral, Inc. ("CaseCentral"), a corporation organized under the laws of the State of California, believes that it would be damaged by registration of the above-referenced mark, and hereby opposes the same. As grounds for its opposition, CaseCentral alleges as follows:

- 1. CaseCentral is a California corporation with its principal place of business at 50 California Street, San Francisco, California 94111.
- 2. Nextpoint is an Illinois corporation with its principal place of business at 4043 North Ravenswood Avenue, Suite 317, Chicago, Illinois 60613.
- 3. CaseCentral is an online litigation support software provider. On August 25, 2008, CaseCentral's Chairman, Christopher Kruse, purchased the internet domain name www.preservationcloud.com.
- 4. In January 2010, Nextpoint, which is also in the online litigation support business, was in the process of developing what it called a "web archiving service that securely captures and indexes data from websites, blogs, Twitter and Facebook feeds"

(the "Archiving Service"). Nextpoint's Archiving Service makes use of "cloud computing," *i.e.*, a means whereby the internet is used to efficiently access processing power and storage on an on-demand basis, to capture and store this data.

- 5. Nextpoint initially contemplated using the www.preservationcloud.com domain name to market the Archiving Service, and calling the product "Preservation Cloud." However, on January 19, 2010, Nextpoint's Chief Executive Officer, Rakesh Madhava, learned that CaseCentral's Christopher Kruse owned the www.preservationcloud.com domain name.
- 6. Nonetheless, apparently hoping Nextpoint could obtain the domain name, on January 28, 2010, Nextpoint applied to the United States Patent and Trademark Office ("USPTO") to register the PRESERVATION CLOUD trademark (the "Mark").

 Nextpoint sought to register the Mark in International Classes 39 and 42. Nextpoint based its application on its alleged intent to use the Mark in commerce, pursuant to 15 U.S.C. § 1051(b). To date, Nextpoint has not filed a statement verifying that it has used the Mark under 15 U.S.C. § 1051(d), and CaseCentral is not aware of any such use. In fact, on information and belief obtained from Nextpoint's own internal e-mails, Nextpoint has no intention of using the Mark.
- 7. On the same date, Nextpoint applied to register two other marks, DISCOVERY CLOUD (Serial No. 77/922,478) and TRIAL CLOUD (Serial No. 77/922,489).
- 8. In or before March 2010, Michael Beumer, Nextpoint's Director of Corporate Communications, attempted to buy the www.preservationcloud.com domain name from CaseCentral's Kruse under false pretenses, by contacting Kruse using

Beumer's wife's e-mail address, and not disclosing Beumer's affiliation with Nextpoint.

Kruse, however, declined.

- 9. Upon learning of this, Nextpoint's CEO, Madhava, decided instead that Nextpoint would purchase the domain name www.cloudpreservation.com, and call the Archiving Service "Cloud Preservation" rather than "Preservation Cloud."
- 10. Accordingly, on April 23, 2010, Nextpoint applied to the USPTO to register the CLOUD PRESERVATION trademark (Serial No. 85/021,489). On June 2, 2010, Nextpoint announced the release of the "beta," or user testing, version of the Archiving Service, under the name "Cloud Preservation" *not* "Preservation Cloud." On August 3, 2010, Nextpoint announced Cloud Preservation's full release.
- 11. On June 8, 2010, Nextpoint filed an action against CaseCentral in the United States District Court for the Northern District of Illinois, *Nextpoint, Inc. v. CaseCentral, Inc.*, Case No. 10-CV-3515 (the "Nextpoint Action"). In that lawsuit, Nextpoint claimed, *inter alia*, that CaseCentral had infringed the Mark by applying to register and using the trademarks EDISCOVERY CLOUD (Serial No. 77/949,557) and CASECENTRAL EDISCOVERY CLOUD (Serial No. 77/949,540).
- 12. On October 27, 2010, the USPTO issued an Office Action refusing to register Nextpoint's proposed DISCOVERY CLOUD and TRIAL CLOUD marks, on the ground that those marks "merely describe[] a function or purpose of [Nextpoint's] goods and/or services," because they describe a process whereby "computer software or cloud will be used in connection with . . . [a] portion of litigation work."
- 13. On November 9, 2010, the USPTO published the Mark in the Trademark Official Gazette. CaseCentral obtained extensions of its time to oppose the registration of the Mark until March 9, 2011.

- 14. On February 16, 2011, Nextpoint filed a motion for voluntary dismissal of the Nextpoint Action. On February 22, 2011, the Court in the Nextpoint Action denied Nextpoint's motion, and ordered that Nextpoint had until March 8, 2011 to opt for either dismissing the action with prejudice or proceeding with the litigation.
- 15. On March 1, 2011, Nextpoint filed a motion for dismissal with prejudice of the Nextpoint Action. The Court granted Nextpoint's motion on March 4, 2011.
- 16. CaseCentral respectfully requests that registration of the Mark be refused on two grounds. *First*, as noted above, Nextpoint applied to register the Mark on the basis that Nextpoint intended to use it in commerce, under Section 1051(b). However, shortly after applying to register the Mark, Nextpoint decided *not* to use the Mark in commerce.
- Archiving Service "Preservation Cloud." However, in or before March 2010, in light of CaseCentral's CEO's ownership of the www.preservationcloud.com domain name, Nextpoint chose to call the Archiving Service "Cloud Preservation" instead. On information and belief, Nextpoint does not use, or plan to use, the Mark to identify any of its other goods or services. Accordingly, registration on an "intent to use" basis under 15 U.S.C. § 1051(b) would be improper.
- 18. Second, under 15 U.S.C. § 1052(e)(1), the Mark does not qualify for registration, because it is merely descriptive of Nextpoint's goods and services. The phrase "Preservation Cloud," as discussed above, merely describes Nextpoint's use of cloud computing for the preservation of certain types of data found on the internet.

 Accordingly, registration of the Mark should be refused, for the same reasons on which

the USPTO previously relied in refusing to register Nextpoint's DISCOVERY CLOUD and TRIAL CLOUD marks.

19. CaseCentral believes it will be damaged if the Mark is registered, because the registration of the Mark will facilitate Nextpoint's assertion of rights under the Mark against CaseCentral, as attempted in the Nextpoint Action and elsewhere, and Nextpoint's claim that CaseCentral is not permitted to use the CaseCentral Marks in commerce. CaseCentral may also be damaged because registration of the Mark may affect CaseCentral's ability to use the www.preservationcloud.com domain name to promote its business.

WHEREFORE, CaseCentral respectfully requests that registration of the Mark be refused.

Date: March 7, 2011

Respectfully submitted,

William J. Frimel

Heffernan Seubert & French LLP

1075 Curtis Street

Menlo Park, CA 94025

Telephone: (650) 322-3048

Facsimile: (650) 322-2976

bill@hsfllp.com

Attorneys for Opposer CaseCentral, Inc.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE TRADEMARK TRIAL AND APPEAL BOARD

) Opposition No. 91198858
)) Mark: PRESERVATION CLOUD
)
) Appl. S/N: 77/922,469
) Filed: January 28, 2010
) Published: November 9, 2010
)

ANSWER TO NOTICE OF OPPOSITION AND AFFIRMATIVE DEFENSES

CaseCentral, Inc. ("CaseCentral"), a corporation organized under the laws of the State of California, believes that it would be damaged by registration of the above-referenced mark, and hereby opposes the same. As grounds for its opposition, CaseCentral alleges as follows:

1. CaseCentral is a California corporation with its principal place of business at 50 California Street, San Francisco, California 94111.

ANSWER: Admitted.

2. Nextpoint is an Illinois corporation with its principal place of business at 4043 North Ravenswood Avenue, Suite 317, Chicago, Illinois 60613.

ANSWER: Admitted.

3. CaseCentral is an online litigation support software provider. On August 25, 2008, CaseCentral's Chairman, Christopher Kruse, purchased the internet domain name www.preservationcloud.com.

ANSWER: Upon information and belief, Paragraph No. 3 is admitted.

4. In January 2010, Nextpoint, which is also in the online litigation support business, was in the process of developing what it called a "web archiving service that securely captures and indexes data from websites, blogs, Twitter and Facebook feeds" (the "Archiving Service"). Nextpoint's Archiving Service makes use of "cloud computing," *i.e.*,

a means whereby the internet is used to efficiently access processing power and storage on an on-demand basis, to capture and store this data.

ANSWER: Applicant admits that it offers a software tool for use in archiving and indexing data from websites, blogs, Twitter and Facebook, that said tool utilizes cloud computing, and that Applicant was developing said tool in January, 2010. Applicant denies any remaining allegations in Paragraph No. 4.

5. Nextpoint initially contemplated using the www.preservationcloud.com domain name to market the Archiving Service, and calling the product "Preservation Cloud." However, on January 19, 2010, Nextpoint's Chief Executive Officer, Rakesh Madhava, learned that CaseCentral's Christopher Kruse owned the www.preservationcloud.com domain name.

<u>ANSWER:</u> Applicant admits that it has contemplated and does contemplate using <u>www.preservationcloud.com</u> in association with its business. Applicant further admits that Christopher Kruse, an individual, presently owns the domain name <u>www.preservationcloud.com</u>, which is parked, and that Mr. Madhava learned of this fact on January 19, 2010. Applicant denies any remaining allegations in Paragraph No. 5, and any inferences Opposer may attempt to draw from the above admissions.

6. Nonetheless, apparently hoping Nextpoint could obtain the domain name, on January 28, 2010, Nextpoint applied to the United States Patent and Trademark Office ("USPTO") to register the PRESERVATION CLOUD trademark (the "Mark"). Nextpoint sought to register the Mark in International Classes 39 and 42. Nextpoint based its application on its alleged intent to use the Mark in commerce, pursuant to 15 U.S.C. § 1051(b). To date, Nextpoint has not filed a statement verifying that it has used the Mark under 15 U.S.C. § 1051(d), and CaseCentral is not aware of any such use. In fact, on information and belief obtained from Nextpoint's own internal e-mails, Nextpoint has no intention of using the Mark.

ANSWER: Applicant admits that it applied for registration of PRESERVATION CLOUD on January 28, 2010 for use in connection with services in classes 39 and 42, admits that said application was filed under Section 1(b), and admits that it has not yet filed a statement

of use with respect to said application. Applicant is without knowledge sufficient to admit or deny what CaseCentral is or is not aware of. Applicant denies any remaining allegations in Paragraph No. 6.

7. On the same date, Nextpoint applied to register two other marks, DISCOVERY CLOUD (Serial No. 77/922,478) and TRIAL CLOUD (Serial No. 77/922,489).

ANSWER: Assuming that "the same date" refers to January 28, 2010, Applicant admits the allegations set forth in Paragraph No. 7. Otherwise, the allegation is denied.

8. In or before March 2010, Michael Beumer, Nextpoint's Director of Corporate Communications, attempted to buy the www.preservationcloud.com domain name from CaseCentral's Kruse under false pretenses, by contacting Kruse using Beumer's wife's email address, and not disclosing Beumer's affiliation with Nextpoint. Kruse, however, declined.

<u>ANSWER:</u> Applicant admits that Mr. Beumer inquired about purchasing the <u>www.preservationcloud.com</u> domain name from Mr. Kruse using his wife's email account and did not mention that he was affiliated with Applicant. Applicant denies any remaining allegations in Paragraph No. 8, and any inferences Opposer may attempt to draw from the above admissions.

9. Upon learning of this, Nextpoint's CEO, Madhava, decided instead that Nextpoint would purchase the domain name www.cloudpreservation.com, and call the Archiving Service "Cloud Preservation" rather than "Preservation Cloud."

<u>ANSWER:</u> Applicant admits that it purchased the domain name <u>www.cloudpreservation.com</u>, and that it uses that domain in association with its business services. Applicant denies the remaining allegations set forth in Paragraph No. 9.

10. Accordingly, on April 23, 2010, Nextpoint applied to the USPTO to register the CLOUD PRESERVATION trademark (Serial No. 85/021,489). On June 2, 2010, Nextpoint announced the release of the "beta," or user testing, version of the Archiving

Service, under the name "Cloud Preservation" — *not* "Preservation Cloud." On August 3, 2010, Nextpoint announced Cloud Preservation's full release.

ANSWER: Applicant admits that it applied to register the mark CLOUD PRESERVATION on April 23, 2010, and admits that it launched a product under its CLOUD PRESERVATION mark on June 2, 2010 for beta testing and on August 3, 2010 as a full release. Applicant denies any remaining allegations in Paragraph No. 10, and any inferences Opposer may attempt to draw from the above admissions.

11. On June 8, 2010, Nextpoint filed an action against CaseCentral in the United States District Court for the Northern District of Illinois, *Nextpoint, Inc. v. CaseCentral, Inc.*, Case No. 10-CV-3515 (the "Nextpoint Action"). In that lawsuit, Nextpoint claimed, *inter alia*, that CaseCentral had infringed the Mark by applying to register and using the trademarks EDISCOVERY CLOUD (Serial No. 77/949,557) and CASECENTRAL EDISCOVERY CLOUD (Serial No. 77/949,540).

ANSWER: Applicant admits that on June 8, 2010, it filed an action against Opposer in the United States District Court for the Northern District of Illinois, *Nextpoint, Inc. v. CaseCentral, Inc.*, Case No. 10-CV-3515. Applicant further admits that it claimed that Opposer infringed its family of Cloud Marks (which were defined to include Preservation Cloud, Discovery Cloud and Trial Cloud) through use of the EDISCOVERY CLOUD and CASECENTRAL EDISCOVERY CLOUD marks. Applicant denies the remaining allegations set forth in Paragraph No. 11.

12. On October 27, 2010, the USPTO issued an Office Action refusing to register Nextpoint's proposed DISCOVERY CLOUD and TRIAL CLOUD marks, on the ground that those marks "merely describe[] a function or purpose of [Nextpoint's] goods and/or services," because they describe a process whereby "computer software or cloud will be used in connection with . . . [a] portion of litigation work."

ANSWER: Applicant admits that the USPTO withdrew its initial approval of Applicant's DISCOVERY CLOUD and TRIAL CLOUD applications and, on October 27, 2010, issued a partial non-final office action under Section 2(e)(1) with respect to the Class 42 services

for each application. Applicant states that said office actions speak for themselves and denies the remaining allegations of Paragraph No. 12.

13. On November 9, 2010, the USPTO published the Mark in the Trademark Official Gazette. CaseCentral obtained extensions of its time to oppose the registration of the Mark until March 9, 2011.

ANSWER: Admitted.

14. On February 16, 2011, Nextpoint filed a motion for voluntary dismissal of the Nextpoint Action. On February 22, 2011, the Court in the Nextpoint Action denied Nextpoint's motion, and ordered that Nextpoint had until March 8, 2011 to opt for either dismissing the action with prejudice or proceeding with the litigation.

ANSWER: Admitted.

15. On March 1, 2011, Nextpoint filed a motion for dismissal with prejudice of the Nextpoint Action. The Court granted Nextpoint's motion on March 4, 2011.

ANSWER: Admitted.

16. CaseCentral respectfully requests that registration of the Mark be refused on two grounds. *First*, as noted above, Nextpoint applied to register the Mark on the basis that Nextpoint intended to use it in commerce, under Section 1051(b). However, shortly after applying to register the Mark, Nextpoint decided *not* to use the Mark in commerce.

ANSWER: Applicant admits that Opposer has requested that registration of Applicant's PRESERVATION CLOUD mark be refused on two grounds, and that one of those grounds is that Applicant applied to register PRESERVATION CLOUD on the basis that it intended to use PRESERVATION CLOUD in commerce, under Section 1051(b), and then shortly after applying to register PRESERVATION CLOUD, Applicant decided *not* to use PRESERVATION CLOUD in commerce. Answering further, Applicant states that this is not a cognizable ground for an opposition, and that an opposition on this ground would be unnecessary because the statement of use requirement would sufficiently protects against

such purported conduct. Furthermore, Applicant specifically denies that it has decided not to use PRESERVATION CLOUD in commerce.

17. As described above, Nextpoint may have initially intended to call its Archiving Service "Preservation Cloud." However, in or before March 2010, in light of CaseCentral's CEO's ownership of the www.preservationcloud.com domain name, Nextpoint chose to call the Archiving Service "Cloud Preservation" instead. On information and belief, Nextpoint does not use, or plan to use, the Mark to identify any of its other goods or services. Accordingly, registration on an "intent to use" basis under 15 U.S.C. § 1051(b) would be improper.

ANSWER: Applicant admits that registration on an "intent to use" basis under 15 U.S.C. §1051(b) would be improper, however notes that *application* on such a basis is not improper. Answering further, Applicant states that registration is and will be proper once Applicant files its statement of use. Applicant denies the remaining allegations of Paragraph No. 17.

18. Second, under 15 U.S.C. § 1052(e)(1), the Mark does not qualify for registration, because it is merely descriptive of Nextpoint's goods and services. The phrase "Preservation Cloud," as discussed above, merely describes Nextpoint's use of *cloud* computing for the *preservation* of certain types of data found on the internet. Accordingly, registration of the Mark should be refused, for the same reasons on which the USPTO previously relied in refusing to register Nextpoint's DISCOVERY CLOUD and TRIAL CLOUD marks.

ANSWER: Denied.

19. CaseCentral believes it will be damaged if the Mark is registered, because the registration of the Mark will facilitate Nextpoint's assertion of rights under the Mark against CaseCentral, as attempted in the Nextpoint Action and elsewhere, and Nextpoint's claim that CaseCentral is not permitted to use the CaseCentral Marks in commerce. CaseCentral may also be damaged because registration of the Mark may affect CaseCentral's ability to use the www.preservationcloud.com domain name to promote its business.

ANSWER: Applicant is without knowledge sufficient to admit or deny whether registration of its PRESERVATION CLOUD mark would affect Opposer's use of "the CaseCentral Marks," as this is an undefined term. Applicant denies the remaining allegations in

Paragraph No. 19. Answering further, Applicant states that Opposer does not own the www.preservationcloud.com domain name and, thus, has no rights that registration could affect. Additionally, Applicant notes that the www.preservationcloud.com domain name has been parked by its owner and is not being used in any manner related to Opposer, let alone as a source identifier for any services offered by Opposer.

AFFIRMATIVE DEFENSES

For its affirmative defense, applicant states as follows:

Affirmative Defense No. 1 – Failure to state a claim

Opposer bases its Opposition on the ground that Applicant has "decided not to use" the

PRESERVATION CLOUD mark after having filed it with the intent to use it. Thus, Opposer

does not allege fraud, because Opposer alleges that Applicant had the requisite intent when it

filed its application and verification statement. Opposer also does not allege non-use, because no

use is required at this point in the application process. Accordingly, Opposer's allegation of its

first ground do not present a recognizable ground for opposition.

Affirmative Defense No. 2 – Unclean Hands

Opposer has unclean hands in that it claims rights to a domain name for purposes of

securing standing that it does not own, and that was only acquired through its agent for purposes

of forestalling Applicant's legitimate use of the PRESERVATION CLOUD mark.

Respectfully submitted,

NEXTPOINT, INC.

Date: April 18, 2011

/John A. Cullis/

John A. Cullis

One of the Attorneys for Applicant

Neal, Gerber & Eisenberg LLP Two North LaSalle Street

Suite 1700

Chicago, IL 60602

(212) 260,000

(312) 269-8000

8

CERTIFICATE OF SERVICE

I, Mike R. Turner, an attorney, state that I deposited a true and correct copy of the foregoing *Answer to Notice of Opposition and Affirmative Defenses* into a U.S. Mail receptacle, postage pre-paid to the following counsel of record on April 18, 2011:

William J. Frimel HEFFERNAN SEUBERT & FRENCH LLP 1075 Curtis St. Menlo Park, CA 94025

> /Mike R. Turner/ Mike R. Turner

NGEDOCS: 1784238.3

Login Sign up





Data Centre Cloud Software Hardware Networks Security Jobs Business Policy Science Odds & Sods Forums Cloud Business Infrastructure Platform SaaS











Archiving and the cloud

SNIA works up some best practices

By Co-chair of SNIA's Cloud Archive & Preservation SIG • Get more from this author

Posted in Infrastructure, 1st November 2011 11:53 GMT

Free whitepaper - AccelOps' Unified Infrastructure Management Examined

Deep dive Cloud is everywhere. Every day we read news about new cloud applications and new cloud providers. But will it really solve all our problems?

When we need more processing power or software services, we use Software as a Service (SaaS) providers. What if we need more storage space? We use Data Storage as a Service (DaaS) providers. It really seems that today's IT issues can be solved by turning to the cloud.

It is simple, less expensive than traditional in-house models and it eliminates the challenge of increasing Π infrastructure costs. Specifically for cloud storage, some studies reveal that it could be up to 75 per cent less expensive than keeping the data in internal storage.

The Storage Network Industry Association (SNIA) defines cloud storage (pdf) as "the delivery of virtualised storage on demand", or "delivery over a network of appropriately configured virtual storage and related data services, based on a request for a given service level." Cloud storage is a fastgrowing business, estimated to reach \$10B by 2014 (pdf).

In addition, organisations are facing growing pressure to store information for long periods of time, generally years. Internal company requirements and compliance regulations introduced by the government such as the Sarbanes-Oxley Act and the Health Insurance Portability and Accountability Act (HIPAA), require companies to keep "cold" data available all the time, with special considerations for data retention, auditing and validation.

The problem is that long-term retention and archiving can be expensive. For the year 2014 it is calculated that over 1 billion diagnostic imaging procedures will be performed in the US, generating about 100PB of data¹. Current backup applications are not suitable for long-term retention and archiving, since they are designed for fast recovery of data and archived data must be retained for

Cloud storage for archiving and long-term preservation

The cost and transfer of IT infrastructure responsibilities to external providers are among the reasons why organisations are moving their archived data to the cloud. Archiving for compliance, e-discovery, application efficiency and email archiving, are additional key drivers for migrating archived organisation data to the cloud.

Consumers are also seeing an increased need for data archiving. With the move to digitisation of information (photos and videos are usually kept in electronic format) the end user's need for storage is also growing quickly. The calculated storage needed for all digital content and associated metadata in 2015 is estimated at a massive 8,000 Exabytes.

Forecasts for 2014 also indicate that cloud archiving will grow between 28-36 per cent per year, the fastest-growing storage service segment after basic cloud storage services 2.

Initially the solution for all these issues seems to be easy: when we need to archive data we move it to a cloud-based archive. However, if we take a closer look the situation is not that simple. The storage of sensitive data in a public cloud requires a series of considerations from different perspectives. Cost, security, availability and integrity of the data are important aspects organisations need to evaluate before selecting a service provider.

Different providers can meet this criterion in different ways so that companies can face the need of migrating their archived data from one provider to another. Data migration also carries a number of

MOST READ MOST COMMENTED

☐ Alert

- VMware rolls up an integrated cloudy control freak
- Love vSphere? You're going to have to love Flash too
- Heroku puffs out Java cloud with oneclick app stack
- Gelsinger wants VMware to be the Apple of the data centre
- AWS adds some CORS blimey to S3







Love vSphere? You're going to have to love Flash too Trevor Pott gets hands-

on with vSphere's new web client

risks for the stored data: the technologies used here can in fact cause corruption due to error rates inherent to the migration. Even data not being migrated can be corrupted via bit-rot, malicious attack or human error.

Long-term preservation and archiving in public clouds also involves the need for a long-term and effective relationship with the provider and this can lead to a number of challenges such as the supplier going out of business, a change of infrastructure and interfaces, cost increase, or the legal restrictions that apply to the geographic storage of data.

Format changes can also represent an obstacle: data stored and archived in a specific format today might not be readable 20 years from now as the technology used to read and interpret the stored bits could disappear.

The need for industry standards

The adoption of an industry standard for cloud storage makes the inter-cloud data migration extremely important. Each provider has its own set of interfaces to store, access, update and delete data and metadata, which means that the end user will have to rewrite the interfaces when migrating between clouds. If customers want to distribute their data across different providers, they need a set of interfaces for each one. A cloud federation approach without a standard interface seems very difficult to follow.

The SNIA's Cloud Data Management Interface (CDMI) standardises the access to data in the cloud via a functional interface used by applications to create, retrieve, update and delete elements from the cloud. CDMI can be implemented on top of the provider's own interface, enabling backwards compatibility with existing interfaces and offering a standardised access to the stored data at the same time.

The CDMI specification uses mostly RESTful principles in the interface design, with some exceptions documented in the specification. Additionally, this interface provides a way to set metadata on containers and their contained data. For archiving and preservation purposes, this metadata is fundamental for fast indexing, searching and information retrieval.

To facilitate the development and adoption of cloud storage SNIA's Cloud Archive & Preservation Special Interest Group (Cloud Archive SIG) has established a list of requirements service providers need to observe to deliver an archive service:

- Multiple primary copies of the data distributed geographically.
- --- CDMI_data_redundancy: the desired minimum number of redundant copies the system needs to maintain.
- --- CDMI_infrastructure_redundancy: the number of independent storage infrastructures supporting the data. Used in combination with the CDMI_data_redundancy, it is used to state that the primary copies for redundancy shall be stored in separate infrastructures.
- Secondary copies (backup)
- --- CDMI_RPO: Used to indicate the desired backup frequency from the primary copies of the data to the secondary copies.
- --- CDMI_RTO: Used to indicate the desired maximum acceptable duration to restore the primary copies from secondary copies.
- Data Validation
- --- CDMI_value_hash: if present, this metadata indicates the hash algorithms and lengths supported.
- Immutability (Data Retention)
- --- CDMI_retention_period: ISO-8601 time interval to specify object retention. When an object is under retention, the object cannot be deleted and its data must remain immutable. Once the retention date expires, the object can be deleted.

How can a cloud user verify that the provider they are considering adheres to these guidelines? And vice-versa, how can a provider communicate to users what is actually being provided? CDMI does this through Capabilities: a type of resource that acts like a service catalogue. When users want to know which level of service the provider offers, they can contact the Capabilities to get a list of Capabilities or functionality delivered.

Through CDMI capabilities, cloud storage providers can specify their level of compliance. In the same way, users can specify the desired level of service.



Face the the future with a private cloud Coping with demand



'Amazon can't do what we do': Twitter-miner's BYO data centre heresy DataSift strains with Hadoop



Bad generator and bugs take out Amazon cloud From failover to fallover



Microsoft: We tried to use Azure ourselves last year, and couldn't But now we're fully ready to cannibalise our own server biz



Start to finish: Building a cloudy service in two weeks

Feature Trevor dons overalls for Microsoft private cloud project



Microsoft assembles a private cloud so you don't have to Trevor's infrastructure drill-down



EMC: Atmos CAN mix an excellent cloudy cocktail You don't node, Nirvanix ...

SPONSORED LINKS

• SQL Storage Compress compresses data by up to 73%

Digital Cloud Archive	Digital Preservation Cloud	Backup Cloud
Retention for extended periods of time	Retention for extended periods of time (indefinitely)	Variable retention periods (may not be long-term)
Permanent Deletion	Permanent Deletion	Incremental Deletion
Long-term information	Long-term information	Data recovery
Availability	Interpretation	Device specific
Interpretation	Authentication	Policies
Authentication		Data protection
Security	Security	Security
Data Integrity	Information Integrity	Data Integrity

Cloud archive and backup capabilities

For archiving purposes, users can establish other requirements, such as encryption and quality-of-service in terms of latency and throughput. Due to regulatory laws and confidentiality of the stored data, customers can also have requirements about geographical placement of the data. For example, cloud storage customers in Europe cannot store certain data outside the European Union.

The SNIA's Cloud Archive SIG is also working to create a description of different profiles for cloud archive and long-term preservation services. This aims to simplify the classification of the services delivered by cloud providers in different profiles like digital cloud archive, digital preservation cloud and backup cloud.

The benefits of industry standards

The adoption of standards by the cloud storage industry will allow vendors and developers to easily integrate with any cloud structure. This integration between heterogeneous systems enables users to migrate their data seamlessly between clouds and cloud storage providers.

A standardised interface for managing the data stored in the cloud will be a differential between vendors in the near future. Forcing the customers to write their own interfaces for each cloud provider will increase the cost and difficulty of cloud archiving adoption and drive customers away from providers with proprietary interfaces.

References

- [1] IEEE. "A Medical Image Archive Solution in the Cloud", 2011
- [2] Forrester Research. "Your Enterprise Data Archiving Strategy", 2011

Bootnote

This article was written by Sebastian Zangaro, Co-chair of SNIA's Cloud Archive & Preservation Special Interest Group. He works for Hewlett-Packard.

For more information on this topic, visit: www.snia.org and www.snia-europe.org.

About the SNIA

The Storage Networking Industry Association (SNIA) is a not-for-profit global organisation, made up of some 400 member companies spanning virtually the entire storage industry. SNIA's mission is to lead the storage industry worldwide in developing and promoting standards, technologies, and educational services to empower organisations in the management of information. To this end, the SNIA is uniquely committed to delivering standards, education, and services that will propel open storage networking solutions into the broader market.

About SNIA Europe

SNIA Europe educates the market on the evolution and application of storage infrastructure solutions for the data centre through education, knowledge exchange and industry thought leadership. As a Regional Affiliate of SNIA Worldwide, we represent storage product and solutions manufacturers and the channel community across EMEA.

The mission of the SNIA Cloud Storage Initiative (CSI) Cloud Archive Special Interest Group (Cloud Archive/Preservation SIG) is to advance the use of public, private and hybrid clouds for archival services and long term retention. We are accomplishing these objectives by promoting the adoption of CDMI and associated standards and by participation in initiatives to educate the community about the benefits of cloud-based services for an archival system. The group's focus includes definitions of best practices and to demonstrate to users, vendors and organisations that the cloud can

be a reliable and trusted partner for archival and long-term retention. For more information about the work for this special interest group, please visit: www.snia.org/cloud/archive.

Free whitepaper - AccelOps' Unified Infrastructure Management Examined

READ MORE Snia Archive Cloud Cloud Storage Share this article

WHITEPAPERS



AccelOps' Unified Infrastructure **Management Examined**

This report provides a current view of AccelOps' capabilities in industry context, including interview excerpts with three AccelOps customers.



Reg Reader Research: SaaS based **Email and Office Productivity Tools**

Read this Reg reader report which provides advice and guidance for SMBs towards the use of SaaS based email and Office productivity tools.

Rate this article



Office 365 in the real world

The Register's Lucy Sheriff is joined by Julian Elve, of The Schools Network, to talk about his recent Office 365 migration.



High Performance for All

While HPC is not new, it has traditionally been seen as a specialist area - is it now geared up to meet more mainstream requirements?

MORE FROM THE REGISTER

Send us News Tips

Week's Headlines

Reg Archive

Top 20 Stories



The Channel Reg Hardware







© Copyright 1998-2012

Privacy Advertise with Us Company Info



Search DLF

ABOUT COMMUNITY

EVENTS

PUBLICATIONS

MEMBERS

FORUMS

2012 FORUM

PAST FORUMS

Forums

2011 DLF Forum

Overview

Call for Proposals

Forum Sponsorship

Schedule

Registration

Travel & Accommodations

2011 Forum Fellows

Forum Ride/Room Share Board

Participants List

2011 Program Committee

Charles Blair Declan Fleming Kevin Hawkins Delphine Khanna Bethany Nowviskie David Reynolds Jenn Riley Melanie Schlosser Sarah Shreeves Joan Starr Jennifer Vinopal Melissa Wisner

Related Links

2012 DLF Forum: Denver, Colorado

2013 DLF Forum: Austin, Texas

Past Forums

Events

Digital Preservation Cloud Services for Libraries and **Archives**

Constellation E: Monday, October 31, 10:30 - 11:15AM

The amount of digital assets, whether born digital or digitized objects from analog and paper artifacts, is growing rapidly. Unlike companies which are required to retain their records for a relatively short period of time to comply with the Sarbanes-Oxley Act, national archives and digital libraries have to face daunting challenges of long-term preservation. Indeed, in order to fulfill the mission to provide discovery and access to digital assets over a long period of time, institutions must develop strategies and mechanisms to effectively preserving these assets. Besides the volume issue, another complicating aspect of digital preservation is data heterogeneity due to the fact that data might originate from various software products specific to diverse application domains. Moreover, organizations have increased their portfolios to disseminate a wide range of file formats from textual documents, geospatial images, audio visual records, web pages, and database files.

Within this context, the question is whether Cloud Computing paradigm can help digital archivists and librarians to meet the challenges of preservation. In recent years, Cloud Computing has gained momentum in the IT world thanks to the maturity of network protocol infrastructure, virtualization technology and a price-based Service Level Agreement structure. At the beginning, research studies have mostly focused on Cloud Storage as a potential service to be used in the digital library and archive community. In this paper, we will study the possibility of using Cloud paradigm throughout all components as specified in the Open Archive Information System (OAIS) reference model, from ingest, storage, data management, preservation, and access. The totality of such services can form what we call Long-Term Digital Preservation as a Service (LDPaaS). We will discuss how the major OAIS functions can leverage LDPaaS strengths, based on the inherent characteristics of elasticity, virtualization, pay-as-you-go resource utilization model of Cloud Services. More interestingly, our argument will show that large institutions have the potential to become LDPaaS providers, and smaller institutions can benefit from the available services. Lastly, we will propose a set of levels of service which can serve as a foundation for LDPaaS service level agreement in terms of ingest processing, preservation processing, and differentiated access capabilities. A Cloud Service, encompassing both storage and preservation of digital objects based on the user's policies for the retention period, preservation level of service, and data confidentiality, can be an attractive alternative to self-provisioning for digital libraries and archives.

Resources

Digital Preservation Cloud Services for Libraries and Archives



<u>((())</u>

View more presentations from qlnguyen

Session Leader

Quyen Nguyen is currently working in the Systems Engineering Division of the ERA Program Management Office at the U.S. National Archives and Records Administration. Before joining the National Archives, he has worked for telecommunications software companies. His experience is in developing software systems for large scale deployment. He has a BS in Computer and Information Science and Applied Mathematics from the University of Delaware and a MS in Computer Science from the University of California at Berkeley.

DLF is a program of the **Council on Library and Information Resources**.

Published by the Digital Library Federation, last modified by **jwinberry** on 29 September 2011. **Some rights reserved. Some notes on privacy.**





Future Evolution of Data Protection is Data Retention and Preservation Cloud, Says Sepaton CEO

by Desire Athow, 07 August, 2008 Page 4

HP selected SEPATON over multiple vendors to be its only VTL provider. A major factor in HP's decision was SEPATON's ContentAware platform.



It differentiates HP's solution as an enterprise-class product and enables innovative, new applications to

be developed, improving disk-based data protection far beyond traditional approaches

7. What technology, service or product has impressed you the most in the past few months?

The Xiotech ISE (Intelligent Storage Element) is very impressive. The ability to condense footprint to that extent at the hardware level is important complementary technology to deduplication in enabling the green data center.

8. What websites/tools I am avid reader of CIO.c within the enterprise data with other vendors and to

We use cookies to improve your online experience. If you continue browsing this site, you consent to these cookies.

ctive on challenges o me in keeping up

Close 9. What's the next big

The future evolution of data protection is the cloud of data retention and preservation - a shared

services model applied to long term storage that is implemented within the enterprise.

Data protection is currently driven by a need from compliance standards (SEC 17A, Sarbanes Ox, etc.), on consequence of jailtime. Moving forward, more sophistication and flexibility will be required.

Business leaders should be able to decide "I want to keep my email for a year, this for 3 years, that for 10, etc." Right now it's difficult to do that as there are no globalized systems.

The data preservation cloud is going to be next big thing and data deduplication helps to make this possible.

10. How do you envision Sepaton's future in the next few years?

We are laser focused on solving real world data storage problems for customers. As a result we expect our revenues to continue growing and for us to continue expanding our business worldwide.

Tags: data management

Most Read



Before and After: What's changed with iOS 6?

IN-DEPTH Software

iOS 6

Prev

Page 4



Apple iPhone 5 preorders now sold out

NEWS Apple

Hot Now



The race to jailbreak the iPhone 5

IN-DEPTH Apple



How to upgrade your iPhone 4S to iOS 6 in four steps

GUIDE Software



iPhone 5 vs Galaxy S3: spec comparison



IN-DEPTH Apple



Display wars: Nexus 7 vs.

Kindle Fire HD

IN-DEPTH <u>Hardware</u>

Recommended Articles



Hands on with the **HTC Windows** Phone 8X and 8S Will Windows Phones make their mark through colour? This week,



Display wars: Nexus 7 vs. Kindle Fire HD When Google launched



LG Optimus G tipped to become the Optimus Nexus?

LG's forthcoming superphone may become the fourth Google-backed Nexus smartphone...



Patent holder Unwired Planet has filed suit against Apple and Google, accusing the firms...

powered by plista

Related Articles



Forefront Identity Manager 2010 R2 Beta Released by Microsoft 03 Aug 2011

Intel Strengthens Data Centre Presence through Fulcrum

Acquisition

22 Jul 2011



Bing Maps Gets Modular Data Centre for Image Processing 29 Jul 2011



Dell Moves Aims To Be More Competitive In The Data Centres Market 09 Jun 2011



16 more related articles...

Latest News



Today's Tech: Fanboys line up for iPhone 5, Apple promises to "improve" maps, BlackBerry service hit with widespread outage

NEWS Mobile & Telco



Is the A6 in the iPhone 5 using a big.SMALL triplecore configuration?

IN-DEPTH Hardware



£500 buys you an Acer Aspire 5755G gaming laptop

DEALS Hardware

0 comments

0 Stars



Leave a message...

Discussion - Con

Community

MEDION

Medion Slimline MD98148 thin-and-light laptop on sale for £299

DEALS <u>Hardware</u>



HTC Windows 8S is cheapest Windows Phone 8 yet with preorder price of £225

DEALS Mobile & Telco

No one has commented yet.

ALSO ON ITPROPORTAL

BT giving away free YouView set top box worth £299 | ITProPortal.com

0 • 1 comment • 5 hours ago



Gareth Pitt-Nash — How does this differ from the BT Vision+ box?

How to upgrade your iPhone 4S to iOS 6 in four steps | ITProPortal.com

0 • 8 comments • a day ago

kam — i updated my phone and then updated my boyfriends phone and all my apps were on his phone plus his p...

iOS 6: mapping out our frustration | ITProPortal.com

0 • 12 comments • a day ago

slow mode m — Maps is the thing I use most and is absolutely a deal breaker. I am forced to buy droid if they don'...

iPhone 5 vs Galaxy S3: spec comparison | ITProPortal.com

3 • 244 comments • 9 days ago

Muz — Was waiting for this launch to upgrade from lphone 4 but i am planning to go for S3 as lphone5 is no...



Follow ITProPortal:



Sign up for ITProPortal news to stay informed:

Your e-mail address

Get updates!

About Us Sitemap Contact Write for Us Advertise Terms and Conditions Feedback Cookie Policy Privacy Settings

© 2008 — 2012 Net Communities. All rights reserved.

Information Playground

Global High-Tech Innovation

<u>About</u>

Archives

Twitter

LinkedIn

CV

November 10, 2009

Research Papers Moving to the Cloud

The <u>ACM</u> has been publishing scholarly works since 1954. They have been diligently maintaining an <u>online library</u> of research papers that has continually benefited the technical community. For years much of their budget has been spent on print-based services as well.

I read an <u>announcement</u> by the ACM last week that they have decided to scale back their investment in print-based services and focus instead on the long-term digital preservation of ACM content as part of a public cloud.

Public clouds that specifically target digital preservation have a different set of requirements than a public cloud like Amazon EC2, for example. The focus in a "preservation cloud" is longevity, and the administrators of said cloud must think like digital curators.

It's an interesting exercise to study the (a) system and (b) curator choices that ACM has chosen. The ACM has chosen to go with <u>CLOCKSS</u> and <u>Portico</u>, respectively. Both CLOCKSS and Portico are not-for-profit organizations.

CLOCKSS

<u>LOCKSS</u> stands for "Lots of Copies Keep Stuff Safe", and the 'C' stands for "controlled". The LOCKSS software framework was developed at Stanford University and is a peer-to-peer, de-centralized model.

The CLOCKSS initiative is run by "the world's leading scholarly publishers and research libraries" with a goal of ensuring "the long-term survival of Web-based scholarly publications for the benefit of the greater global research community". CLOCKSS ingest boxes are located at Rice, Indiana, and Stanford university. As libraries and researchers submit content to these "ingest boxes", they are stored in normalized, maintainable format in triplicate across the sites. Once all of the ingest boxes have cross-audited the content, the artifacts are moved to "archive nodes" spread throughout the globe. These boxes continually audit themselves and verify the authenticity of the content, and create new versions when hardware fails (very similar to a <u>RAIN</u> architecture).

Interestingly enough, the solution is a "dark archive". The initial content is not accessible to the general public. The ingest and preservation within CLOCKSS is initially focussed on maintaining content for the long-term. When a "trigger event" occurs, however, content is made public by migrating it to the newest format and storing it on publicly available nodes at Stanford and the University of Edinburgh.

A description of how CLOCKSS works can be found here.

Portico

Portico can be thought of as a third-party partner that supplies the people and processes behind the CLOCKSS solution. The best way to explain the process they bring to the table can be found in one of their <u>brochures</u>:

PORTICO MANAGED PRESERVATION



Source files undergo numerous processing steps to identify, classify, and validate.



Convert or "normalize" XML files to NLM Archiving and Interchange document type definition (DTD), if necessary.



Apply metadata wrapper based on Metadata Encoding and Transmission (METS) standard and PREMIS.



Perform quality control and create standard archival package.



Deposit package in archive management system.

 $Diagram\,from\,the\,\,\underline{Portico\,brochure}$

The CLOCKSS and Portico solution relies heavily on migration of data formats as the years roll by. I've always wondered about the feasibility of such an approach. Can it scale to billions of documents? Does the system have to continually upgrade all documents to newer file formats as these new formats become available? One thing I picked up as I learned about their solution is that the format conversion occurs when the format goes from "dark" to "publicly available". In other words, there's no need to continually upgrade file formats.

The alternate approach to format conversion is something I've been researching here at EMC. As an entire class of documents is imported into an archive, can a Virtual Machine also be imported that is able to "read" all of these documents, both now and in the future? This would require some time of virtual machine "player" that has infinite playback capability (no easy task).

I hope to learn more about the server/storage implementation of CLOCKSS at locations around the world.

Steve

http://stevetodd.typepad.com

Twitter: @ SteveTodd EMC Intrapreneur

Posted at 08:13 AM in <u>Digital Preservation</u> | <u>Permalink</u>

Technorati Tags: ACM, CLOCKSS, digital curation, digital preservation, Portico

TrackBack

TrackBack URL for this entry:

http://www.typepad.com/services/trackback/6a00e5500d490088340128756fc5c5970c Listed below are links to weblogs that reference Research Papers Moving to the Cloud:

Comments

 ${\color{red} extstyle extst$

The comments to this entry are closed.

PLUS ULTRA: THIRD-PARTY PRESERVATION IN A CLOUD COMPUTING PARADIGM

Joseph A. Nicholson*

I. INTRODUCTION

"This is a story about control . . . to get what I want. Control. I have to have a lot."

- Janet Jackson

A natural disaster strikes and, eventually, a devastated homeowner is visited by an insurance adjuster. Though the insurer typically requires the insured to submit a formal request, the claims adjuster assures the homeowner that he will file the request on her behalf. On his way to the next insured, the adjuster enters notes about his meeting onto a remote server through his handheld PDA. Ultimately, the adjuster is consumed with other potential claims and forgets to file their claim. The insurer refuses to pay and the insured files suit, claiming promissory estoppel and detrimental reliance.

During discovery, the plaintiff learns of the electronic notes created by the adjuster and requests a copy. But the insurer does not retain copies of this class of data in its own possession. As part of a growing trend towards cost-cutting and other efficiencies, it has rented large amounts of server space to store and process this type of information, and to provide the very mobility that allowed the adjuster's timely visit. Now faced with a formal production request, the insurer learns the notes are nowhere to be found. As far as can be determined by the remote computing service provider, the file was accidentally mislabeled and is deleted or lost. Or, says the vendor, it might have been located on a server that was recently seized by federal agents in an unrelated matter.¹ No matter what the cause, the insurer

^{*} J.D. Candidate, 2012, University of California, Hastings College of the Law. This work would not have been possible without the patience and insight of Professor Richard Marcus and Chris Mammen, for which the author is most appreciative. Special thanks are also due to Emily A. Cobb of Ropes & Gray LLP, and Vicki Clewes, both of whom gave graciously of their valuable time and considerable knowledge.

^{1.} Or perhaps imagine instead that the complaint includes allegations of fraud and unfair business

cannot produce the requested record because it is simply gone. 2 It has been spoliated. 3

Who is to blame in this scenario? Who was in control of the lost information? What, if anything, can be inferred from the disappearance of the evidence? Who, if anyone, gets sanctioned for its spoliation? Can the nonparty cloud computing vendor be sanctioned? Or should the plaintiff's case be dismissed because she cannot establish the existence of a promise? Should the defendant or the defendant's counsel be sanctioned instead?

The duty of a party to preserve potentially relevant information attaches at the point at which litigation becomes reasonably foreseeable, meaning the duty for a party can arise years before litigation actually commences. But when that party's information is stored remotely on the servers of a vendor, the typical expectations of preservation take on new and challenging dimensions. How effectively can outside counsel devise, and in-house counsel enforce, a litigation hold for data stored in the cloud? How costly is it to search the cloud for potentially relevant information and purchase new space on which to segregate it? How burdensome is it to monopolize bandwidth and processing capacity to download the data for local storage?

As information and, presumably, responsive documents increasingly move into the actual custody of third parties, the business community and the legal system will face the reality that third-party computer systems not only multiply the number of documents and copies that are created and retained, but also inadvertently destroy, alter, or misplace information. Just as the technical uniqueness of electronically stored data must be recognized in fashioning controlling discovery standards, so too should sanctions be tailored to the electronic context if the values sought to be furthered by

practices against various employees and executives of the insurer. A copy of the adjuster's note referring to his promise has been produced, but a reliable version of the metadata that would prove which employees accessed the notes and when, cannot be found or simply does not exist.

nı

192

^{2.} A further complication would arise if the only remaining evidence of the adjuster's notes was information about his access to the cloud that existed as proprietary data created by the vendor. The record could be enough to justify an adverse inference against the insurer, but its discovery might be opposed by the vendor as confidential. This could be complicated further still if the proprietary record was not possessed by the vendor but another third-party company providing services directly through the vendor's platform.

^{3.} Spoliation refers to the destruction or material alteration of evidence or to the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation. Pension Comm. of Univ. of Montreal Pension Plan v. Banc of Am. Sec., 685 F. Supp. 2d 456, 465 (S.D.N.Y. 2010) [hereinafter *Pension Committee*]; Silvestri v. Gen. Motors Corp., 271 F.3d 583, 590 (4th Cir. 2001). Though some prefer to use "spoliation" purely for the destruction of evidence, the definition in *Pension Committee* would seem to include scenarios in which evidence is not produced because it cannot be identified through reasonable means and those in which the data has lost its probative value for having been materially altered by automatic electronic processes.

^{4.} Zubulake v. UBS Warburg L.L.C., 220 F.R.D. 212, 216 (S.D.N.Y. 2003).

^{5.} Micron Tech., Inc. v. Rambus Inc., 255 F.R.D. 135, 148 (D. Del. 2009).

litigation are to be respected.⁶ Unless cloud service providers accept a particular contractual obligation to preserve information in dispute, they are likely to escape repercussions from the destruction of the crucial data even when they are the key player in its loss. Both the party contracting with the vendor and their opposition have a stake in preventing this undermining of the basic truth-finding goal that is the foundation of the litigation process.⁷

After amending the discovery rules in 2006, rulemakers are considering further changes and at least one magistrate judge has emphasized the need for any new e-discovery rule to be forward-looking enough to anticipate the cloud computing environment.⁸ In the current absence of such a preservation rule, however, this note outlines some of the currently existing means by which businesses and their counsel can approach preservation of ESI in the cloud when needed for litigation. Section II provides an overview of the cloud computing paradigm and the emergence of third parties as the actual and practical custodians of data. The third section outlines some of the basic challenges to discovery in the cloud, where litigants simply have less practical control of data than they might otherwise have if the information was stored locally or in hard copy. This section examines how current litigation tools aimed at compelling production by third parties have little use in encouraging preservation. Finally, section IV discusses how terms of service agreements can ease some of the tension, but typically only at the cost of essential cloud computing benefits, and previews some implications of applying the principle of proportionality in preservation.

II. PRESERVATION CHALLENGES OF THE CLOUD COMPUTING PARADIGM

In rejecting an independent tort of spoliation against parties to an underlying lawsuit in California, the state's Supreme Court said in 1998 that non-tort remedies for spoliation were apparently effective since "the problem of spoliation does not appear to be widespread." But it appears that, as technological advances in electronically stored information ("ESI")

^{6.} H. Redish, *Electronic Discovery and the Litigation Matrix*, 51 DUKE L.J. 561, 619 (2001). According to renowned author and futurist Bruce Sterling, electronic storage is unique in that it is "inherently unstable." Kari Kraus, *When Data Disappears*, N.Y. TIMES, (Aug. 6, 2011), http://www.nytimes.com/2011/08/07/opinion/sunday/when-data-disappears.html?_r=1.

^{7.} See Redish, supra note 6, at 600; FED. R. CIV. P. 1 (the resolution of every action should be "just").

^{8.} E-Discovery: Discussion of the Cost Benefit Analysis of E-Discovery and the Degree to Which the New Rules are Working or Not, CIVIL LITIGATION CONFERENCE (May 11, 2010) (downloaded using RealPlayer) (Magistrate Facciola dedicating his remarks to the singular point that the cloud computing paradigm represents the future of information technology and e-discovery and that, therefore, any new preservation rule must be designed for and tested against this emergent reality).

^{9.} Cedars-Sinai Med. Ctr. v. Super. Ct., 954 P.2d 511, 518 (1998).

Vol. 8:1

have revolutionized business, they have also exacerbated a once judicially manageable problem into a challenge of entirely new proportions. Just twelve years later, Judge Rosenthal of the Southern District of Texas began his exposition on the topic in Rimkus Consulting Group, Inc. v. Cammarata by stating, "[s]poliation of evidence—particularly of electronically stored information—has assumed a level of importance in litigation that raises grave concerns." Indeed. A study presented at the 2010 Civil Litigation Conference and published in the Duke Law Journal found that there were more e-discovery sanctions cases in 2009 than in all years prior to 2005 combined.¹¹ The same study identified a total of 230 sanctions awarded just for spoliation of ESI in the federal court system before the start of 2010.¹² Though Gibson, Dunn, & Crutcher reports that fewer of the total ediscovery sanctions sought in 2010 were granted than in 2009, ¹³ the first half of 2011 nevertheless saw a particularly brow-raising sanction awarded for egregious e-discovery abuse¹⁴ and something approaching a "three strikes" rule for bad faith failure to disclose. 15 Another recent survey shows Facebook is a source of evidence in one of every five divorce cases. 16 A report by Deloitte finds that lawyers expect e-discovery will be even more challenging in the near future, 17 suggesting this is not the end, nor even the beginning of the end of our grappling with e-discovery, but perhaps the end of the beginning.

^{10.} Rimkus Consulting Group, Inc. v. Cammarata 688 F. Supp. 2d 598, 607 (2010).

^{11.} Dan H. Willoughby et al., Sanctions for E-Discovery Violations: By the Numbers, 60 DUKE L.J. 789, 794 (2010).

^{12.} Id. at 790.

^{13. 2010} Year-End Electronic Discovery and Information Law Update, Gibson, Dunn & CRUTCHER (Jan. 13, 2011), http://www.gibsondunn.com/Publications/Pages/2010YearEndE-Discovery-InformationLawUpdate.aspx.

^{14.} Green v. Blitz U.S.A., Inc., No. 2:07-CV-372 TJW, 2011 WL 806011, at *10-11 (E.D. Tex. Mar. 1, 2011) (defendant ordered to pay \$250,000 civil contempt fine as well as provide copy of sanctions order to every plaintiff in a proceeding against it for the previous two years and to file a copy of the order in every case brought before the court in the next five years.).

^{15.} Lee v. Max Int'l, L.L.C., 638 F.3d 1318, 1321 (10th Cir. 2011) ("[A] party's thrice repeated failure to produce materials that have always been and remain within its control is strong evidence of willfulness and bad faith, and in any event is easily fault enough, we hold, to warrant dismissal or default judgment.").

^{16.} Facebook Fueling Divorce, Research Claims, TELEGRAPH, (Dec. 21, 2009, 1:02 PM) http://www.telegraph.co.uk/technology/facebook/6857918/Facebook-fuelling-divorce-research-claims. html; Big Surge in Social Networking Says Survey of Nation's Top Divorce Lawyers: Facebook is Primary Source for Compromising Information, AM. ACAD. OF MATRIMONIAL LAWYERS, (Feb. 10, 2010) http://www.aaml.org/about-the-academy/press/press-releases/e-discovery/big-surge-social-net working-evidence-says-survey-.

^{17.} E-Discovery: Mitigating Risk Through Better Communication, DELOITTE (2010), http://www.deloitte.com/assets/DcomUnitedStates/Local%20Assets/Documents/FAS_ForensicCenter_us_fas-us_dfc/us_df

Winter 2012

THIRD PARTY PRESERVATION

195

A. THE CLOUD COMPUTING PARADIGM

Waxing philosophical in the famous case of Zubulake I, District Judge Shira Sheindlin noted, "The world was a far different place in 1849, when Henry David Thoreau opined (in an admittedly broader context) that '[t]he process of discovery is very simple." ¹⁸ Unfortunately for litigants, their counsel, and the courts, the world is a very different place today than it was in 1999 or in 2003—and it is likely to be significantly more different five or ten years into the future. For one thing, the backup tapes that are seemingly ubiquitous in the e-discovery disputes of just five or ten years ago, though still in use, have been superseded by CD-ROM, DVD, Blue-Ray, hot-swappable flash drives and, increasingly, online backup. ¹⁹ While not new, the emergence of cloud computing in particular represents a paradigm shift²⁰ that has already revolutionized social networking and is forecast to have a profound ongoing impact on IT organizations, 21 law firms and corporate law departments, 22 health care providers, 23 and the corporate world in general.²⁴ The increasing functionality of the Internet is decreasing the role of the personal computer, which is reversing the trend towards a decentralized computing environment.²⁵ In the words of CNET News Editor in Chief Dan Farber, 2008 marked only the beginning of "the age of planetary computing" in which "billions of people will be wirelessly interconnected" by a "massive scale, brutally efficient cloud-based infrastructure."26

^{18.} Zubulake v. UBS Warburg LLC, 217 F.R.D. 309, 311 (S.D.N.Y. 2003).

^{19.} George Ou, Are Tape Backup Systems Obsolete?, ZDNET (July 10, 2006), http://www.zdnet.com/blog/ou/are-tape-backup-systems-obsolete/267; Maxim Yurin, The History of Backup, SOFTLOGICA http://www.backuphistory.com/ (last visited Sept. 22, 2011); see also E-Discovery: Discussion of the Cost Benefit Analysis of E-Discovery and the Degree to Which the New Rules are Working or Not, supra note 8.

^{20.} Enterprise Cloud Services: Deriving Business Value From Cloud Computing, WHITE PAPER (2008) available at http://cloudservices.microfocus.com/main/Namespaces/MFECS/doc/MFECS-WP-deriving-business-value.pdf; Venkat Rangan, E-Discovery and the Cloud: The Duty to Preserve Electronically Stored Information (ESI), E-DISCOVERY 2.0 (May 28, 2010), http://www.clearwellsystems.com/e-discovery-blog/2010/05/28/e-discovery-and-the-cloud-the-duty-to-preserve-electronically-stored-information-esi/.

^{21.} Michael Biddick, *Why You Need a SaaS Strategy*, INFO. WEEK (Jan. 16, 2010), http://www.informationweek.com/news/services/saas/showArticle.jhtml?articleID=222301002.

^{22.} David Narkiewicz, Legal Tech Forecast: Cloudy, With Only a Chance of Purchasing New Software, 32 PA. LAW 56, 56 (2010).

^{23.} Chris Chatman, How Cloud Computing is Changing the Face of Health Care Information Technology, 12 No. 3 J. HEALTH CARE COMPLIANCE 37, 37-38 (2010).

^{24.} William R. Denny, Survey of Recent Developments in the Law of Cloud Computing and Software As a Service Agreement, 66 Bus. LAW 237, 242 (2010).

^{25.} William J. Robison, Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act, 98 GEo. L. J. 1195, 1199–1200 (2010).

^{26.} Bill Farber, Cloud Computing Hangover, CNET NEWS (June 26, 2008 10:35 AM), http://news.cnet.com/8301-13953_3-9978153-80.html.

Vol. 8:1

The quintessential feature of cloud computing is that, rather than storing data on an individual computer or in onsite backups, high-speed Internet access is used to outsource this service, often to third-party providers. In cloud computing, the user's individual computer accesses the cloud through the Internet in a manner reminiscent of the way a "dumb terminal" is used to access a mainframe. In a growing number of companies, employees are no longer the custodians of the records they produce—from their desks, laptops or handheld devices they access and manipulate documents and records that are stored remotely on third-party servers.

This cloud computing paradigm has emerged against a backdrop in which the federal courts have become increasingly attentive to the novel issues e-discovery creates in litigation. But despite the prodigious efforts already made by courts, individual judges, scholars and rulemaking bodies, third-party spoliation has been a relatively undeveloped area of e-discovery that seems to only now be receiving the serious attention it deserves.³⁰ Though the consequences of this oversight to date may be limited, it is particularly alarming given not just the proliferation of ESI, but the increasing rate at which potentially relevant and discoverable ESI will be in the hands of third-party service providers. As currently understood, parties to litigation are deemed to be in "control" of information to which they have access or the legal right to obtain, even if it is actually in the

^{27.} Clouds can be either internal or external, and each type can further be classified as private, essentially an intra-net, or community-based, with access limited to specific groups or individuals. For this article, "cloud computing" will typically refer to public clouds in which third parties provide cloud computing services to businesses and the general public. See Peter Mell & Tim Grance, Effectively and Securely Using the Cloud Computing Paradigm, slide 11 (Mar. 13, 2009), http://csrc.nist.gov/organizations/fissea/2009-conference/presentations/fissea09-pmell-day3_cloud computing.pdf.

^{28.} Robison, *supra* note 25, at 1199–1200.

^{29.} The precise definition of "custodian" in this context is "somewhat tricky." *Agenda for April* 2011 *Meeting*, CIVIL RULES ADVISORY COMM., 12 (2011) *available at* http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/Agenda%20Books/Civil/CV2011-04.pdf. And what responsibilities are involved is troubling and convoluted in its own right. In the context of cloud computing, "custodian" can refer to the employee who creates and routinely access a file or the third-party storing it. To the extent that cloud service providers attempt to completely disavow any responsibility for preservation in their terms of service, service providers are probably best described as having possession of the ESI, while the employee or the party is charged with the preservation obligations of a custodian. This framework, however, still leaves open the question of control, which is from a practical perspective, probably the most significant.

^{30.} See, e.g., Greyhound Lines, Inc. v. Wade, 485 F.3d 1032, 1035 (8th Cir. 2007) (no sanction for third-party spoliation where intentional destruction is the requisite level of culpability). At least one commentator has observed an emerging consensus that the 2006 Amendments inadequately addressed the problems associated with e-discovery and that a rule addressing preservation and spoliation would be "a valuable addition to the Federal Rules." See Thomas Y. Allman, Achieving a More Rational Treatment of Preservation Obligations: The Need to Amend The Federal Rules (Again), in ELECTRONIC DISCOVERY GUIDE 2010, at 140 (PLI Litig. & Admin. Practice, Course Handbook Ser. No. 23262, 2010). Discussion of such a rule was placed on the April 2011 agenda of the Civil Rules Advisory Committee. Agenda for April 2011 Meeting, supra note 29, at 205.

possession and custody of a third party.³¹ The traditional custodian is often the employee or agent of the party who creates and accesses ESI locally, and therefore stores and preserves a record. Barron's legal dictionary suggests the word specifically implies not ownership, but a "keeping, guarding, care, watch, inspection, preservation or security of a thing."³² Though the law does not recognize a vendor's duty to preserve data in its custody apart from the terms of service under which its services are offered, the nature of cloud computing appears to put the vendor in a position superior to the traditional custodian in terms of preservation and control.

One of the very reasons that the Internet was early depicted as a cloud is that, while it creates the potential to access a wide variety of interconnected resources, it also obscures what is available.³³ Far from the literal "series of tubes" the Internet has been imagined to be, the very concept of network infrastructure is something of an abstraction based on complex interactions between servers, applications, data and heterogeneous platforms.³⁵ For example, mature cloud computing services employ a feature called multi-tenancy, which means that one application instance may be serving hundreds of companies simultaneously.³⁶ Rather than the service provider customizing an application, each user customizes their access via metadata.³⁷ While the fact that ESI is often recorded in multiple locations and in more than one medium may make it relatively rare that a particular piece of discoverable information is only available as ESI from a third party, locating and distinguishing and authenticating duplicate or slightly different versions typically occurs with considerable difficulty and expense.38

^{31.} See Victor Stanley, Inc. v. Creative Pipe, Inc., 269 F.R.D. 497, 523–24 (D. Md. 2010).

^{32.} BARRON'S LAW DICTIONARY 133 (6th ed. 2010). The Latin root *custodia* could refer to both a physical container in which something was placed for safekeeping or to the care itself shown towards the object.

^{33.} Mell & Grance, supra note 27, at slide 7.

^{34.} The phrase was famously coined by Sen. Ted Stevens on June 28, 2006, in a speech opposing net neutrality. Ted Stevens, Speech Regarding Net Neutrality (July 28, 2006), available at http://www.youtube.com/watch?v=f99PcP0aFNE. The phrase was mocked by Jon Stewart on The Daily Show roughly two weeks later. The Daily Show With John Stewart (Comedy Central Television broadcast July 12, 2006), available at http://www.thedailyshow.com/watch/wed-july-12-2006/headlines---internet. For a measured defense of Stevens, see Ed Felten, Taking Stevens Seriously, Freedom to Tinker (July 17, 2006, 7:21 AM), http://www.freedom-to-tinker.com/blog/felten/taking-stevens-seriously.

^{35.} Mell & Grance, *supra* note 27, at slide 7.

^{36.} *Id.* at slide 39.

^{37.} *Id*.

^{38.} Brandon M. Kimura & Eric K. Yamamoto, *Electronic Discovery: A Call For a New Rules Regime For the Hawaii Courts*, 32 U. HAW. L. REV. 153, 161 (2009); *but see Cryptographic Hash Algorithm Competition*, NAT'L INST. OF STANDARDS AND TECH. (Dec. 15, 2005), csrc.nist.gov/groups/ST/hash/sha-3/index.html. The reduction of digital documents and images to a series of hash values that can be summed to produce a unique identifying value is a likely way that seemingly similar

The term "cloud computing" is a visual metaphor that conveys the versatility of the Internet.³⁹ The Internet is in fact the quintessential cloud computing service, consisting of a group of computer servers linked together and functioning as a single "cloud" of resources.⁴⁰ essentially, the cloud computing paradigm is nothing more than the realization of the Internet's full potential. Today, cloud computing services leverage international networks of computing resources, including applications, processing, storage, technical support, and technical infrastructure, with the result that data stored "in the cloud" can be located anywhere in the world and even shifted amongst servers depending on immediate demands.41 In a 2011 survey of over 500 IT professionals, CTOs and developers, forty percent to fifty percent indicated current use of cloud-based solutions for product test and development, operation of data centers, increasing office productivity and email.⁴² It will not be uncommon for a business or government agency to operate a call center staffed by employees who were selected through Internet staffing agencies like Salesforce.com, who access customer records stored on distant servers via Internet and who manipulate those records or create new ones that will also be stored remotely. The traditional notion that these operators are the ultimate custodians of these records seems inaccurate and unhelpful.

B. RISE OF THE THIRD-PARTY CUSTODIAN

If cloud computing is the way of the future, then that future will be a world in which much discovery involves "documents" in the custody of nonparties. While uniform definitions are elusive, ⁴³ cloud computing typically refers to data and software applications that are stored in cyberspace on remote servers, rather than on the servers or PCs of the firms that use them. ⁴⁴ Subsets of cloud computing include "software as a service" ("SaaS"), "infrastructure as a service" ("IaaS"), "platform as a service" ("PaaS"), and the perhaps more familiar social networking services of Web 2.0.⁴⁵ The essence of all forms of cloud computing is that the service provider allows its users to do their processing and storage of

pieces of ESI will be quickly distinguished or identified in the near future. Such algorithmic approaches, however, will probably not obviate the need for a document-by-document evaluation of similar electronic documents and evaluation of the differences in terms of relevance.

- 39. Mell & Grance, supra note 27, at slide 7.
- 40. Robinson, supra note 25, at 1199.
- 41. Barry Reingold & Ryan Mrazik, Cloud Computing: The Intersection of Massive Scalability, Data Security and Privacy (Part I), 14 No. 5 CYBERSPACE LAW. 1, 1 (2009).
 - 42. Cloud Survey Results, GOGRID, 6 (2011), http://go.gogrid.com/2011_survey_results.
- 43. Denny, supra note 24, at 237; Narkiewicz, supra note 22, at 56; Cloud Survey Results, supra note 42, at 3.
 - 44. Narkiewicz, supra note 22, at 56.
 - 45. Reingold & Mrazik, supra note 41, at 1.

Vol. 8:1

information on its servers—reliance on the Internet to satisfy the computing needs of end users is the hallmark of the cloud computing paradigm.⁴⁶

At the same time, these resources are massively scalable, meaning they can be custom fit to provide virtually any computing service needed.⁴⁷ Users can buy as much or as little computing, storage, processing and development power as they need without actually owning any of the hardware, software or technology expertise.⁴⁸ SaaS is already used for a variety of computing tasks, such as running spreadsheets, hosting websites, producing and keeping payroll records, compiling and storing data, and word processing.⁴⁹ PaaS and IaaS allow users to write software applications on a hosted web platform and rent network capacity, respectively.⁵⁰

While this outsourcing of computing and storage presents obvious security challenges, its numerous advantages outweigh the risks for a growing number of businesses. Cloud computing has lower capital costs than on-site storage and computing, is quick and cheap to setup, and allows for employee mobility by making applications available at remote offices, on the road, via a smartphone, or from a home PC.⁵¹ And though cloud computing is currently far from universal, it is difficult to imagine that the future workplace will not include a variety of cloud computing features. Already, about three-fourths of companies using SaaS consider these applications "extremely important" and about one-third describe them as "mission critical." The scalability and pay-as-you-go features of cloud computing make it "cash-flow-friendly," an important factor in economic conditions where up-front funding is more difficult to obtain.⁵³

To further compound the implications for e-discovery, government agencies are also implementing cloud computing technology to comply with mandates to cut costs and increase transparency—and they are advocating similar adoptions by private sector organizations.⁵⁴ In particular, the Department of Health and Human Services has already begun actively promoting and supporting a nationwide upgrade of health IT infrastructure by distributing grants for the creation of electronic health

^{46.} Richard Stallman, Who Does That Server Really Serve?, Boston Review (Mar. 18, 2010), http://bostonreview.net/BR35.2/stallman.php; Enterprise Cloud Services: Deriving Business Value From Cloud Computing, supra note 20.

^{47.} Reingold & Mrazik, supra note 41, at 1.

^{48.} *Id*.

^{49.} Id. at 2; Stallman, supra note 46.

^{50.} Reingold & Mrazik, *supra* note 41, at 1–2.

^{51.} Biddick, supra note 21; Chatman, supra note 23, at 37-38.

^{52.} Biddick, supra note 21.

^{53.} Enterprise Cloud Services: Deriving Business Value From Cloud Computing, supra note 20.

^{54.} Chatman, supra note 23, at 37-38.

records ("EHR") systems.⁵⁵ Another emerging technology trend at least tangentially related to cloud computing also suggests probative information will be increasingly concentrated in the possession of companies or other organizations that will not necessarily be the parties to the dispute in which the information is relevant. So called "smart grid" technology in some states, like California, concentrates the end consumers' energy usage data in the utility company itself.⁵⁶ Because smart meters gather information about an individual home or locale's energy consumption virtually in real time, the ability to process and interpret the data gives unprecedented access into one of the traditionally most private spaces in life.⁵⁷ In other states, utilities are teaming with telecom companies who provide broadband transmission capacity and other edge services that require them to either purchase or directly gather data from electricity consumers.⁵⁸ In either event, it is already foreseeable that such information will be relevant in a variety of civil and criminal cases.⁵⁹

For many individuals, however, social networking sites like Facebook, Twitter, and YouTube are probably the most recognizable facet of the cloud computing paradigm. Any lingering doubts about the viability of such ventures as legitimate, for-profit enterprises should be put to rest by Goldman Sachs's attempt to raise \$1.5 billion in financing for Facebook, making it arguably "the hottest property on the planet," and a similar \$1.1 billion venture fund implemented by JPMorgan & Co. In 2011, Twitter and Salesforce.com alone are expected to rent a combined 400,000 square feet of San Francisco office space, helping the vacancy rate in the City by

^{55.} Chatman, supra note 23, at 38.

^{56.} How the SmartMeterTM System Works and What It Can Do for You, PG&E.COM, http://www.pge.com/myhome/customerservice/smartmeter/facts/ (last visited Mar. 2, 2011).

^{57.} Jennifer Lynch & Lee Tien, Joint Comments of the Center for Democracy & Technology and the Electronic Frontier Foundation on Proposed Policies and Findings Pertaining To The Smart Grid 1, 4-9 (2010) *available at* https://www.eff.org/files/CDTEFFJointComment030910.pdf.

^{58.} See Cynthia J. Larose, Energy and Clean Technology Alert: Smart Grid Privacy Issues To Be Examined by the Federal Communications Commission – Comment Period through October 2, 2009, MINTZ LEVIN (Sep. 25, 2009), http://www.mintz.com/publications/1954/Energy_and_Clean_Technology_Alert_Smart_Grid_Privacy_Issues_To_Be_Examined_by_the_Federal_Communications_Commission_Comment_Period_through_October_2_2009; Jesse Ward, The Smart Grid Primer: Building the Smart Grid Broadband Network, NATIONAL TELECOMMUNICATION COOPERATIVE ASSOCIATION (Aug. 23, 2010), http://www.ntca.org/new-edge/epapers/the-smart-grid-primer-building-the-smart-grid-broadband-network.

^{59.} Lynch & Tien, *supra* note 57, at 4–9.

^{60.} For example, in July 2010 Facebook exceeded 500 million active users, well in excess of the total population of the entire United States. *See Company Timeline*, FACEBOOK, http://www.facebook.com/press/info.php?timeline (last visited Mar. 2, 2011).

^{61.} Dominic Rushe, *Goldman Sachs Suffers Facebook Fiasco*, GUARDIAN (Jan. 17, 2011, 9:41 p.m.), http://www.guardian.co.uk/business/2011/jan/17/goldman-sachs-facebook-private-placement; Dan Levy & Ari Levy, *Twitter Boosts San Francisco Offices as Banks Give Up Space*, BLOOMBERG (Mar. 02, 2011, 4:58 p.m.), http://www.businessweek.com/news/2011-03-02/twitter-boosts-san-francisco-offices-as-banks-give-up-space.html.

201

the Bay drop faster than any other in the country.⁶²

Unlike much of the ESI of just a few years ago, information created by users of social networks is often not stored permanently on a user's computer, but rather on the social network's own servers. As of 2009, Facebook utilized 30,000 servers in several different data centers, handling the equivalent of 1,000 times the volume of mail delivered daily by the U.S. Postal Service, according to its Vice President of Technology. Twitter similarly maintains a 15,000-square-foot data center to accommodate the upwards of 90 million "tweets" sent daily via its networks. Though some data, such as the 80 billion pictures more or less permanently stored by Facebook may be available through other reasonably accessible means, other content, particularly data generated on the networking site rather than simply uploaded to it, is probably no more than ephemeral data on the user's own computer.

Information generated on social networks has already been used in family law for divorce and child welfare cases, in employment law cases, and in the damages phases of other civil litigation. For example, photos deleted from a Facebook account became the focus of a heated discovery dispute in a 2010 Virginia case for wrongful death and resulted in an adverse inference sanction for spoliation. In late 2009, a teenager in New York was released after twelve days in prison, and robbery charges against him were dropped, once his family produced a time-stamped Facebook status update that convinced police of his innocence—but not before the date and time of the update were confirmed by Facebook pursuant to a Brooklyn Assistant District Attorney's subpoena. Though the implications of the cloud computing paradigm for criminal law are beyond the scope of this work, the example of the so-called "Facebook alibi" illustrates a central point—that crucial evidence will increasingly be in the

^{62.} Levy & Levy, supra note 61.

^{63.} Andrew C. Payne, Note, Twitigation: Old Rules in a New World, 49 WASHBURN L.J. 841, 848 (2010)

^{64.} Payne, supra note 63, at 848.

^{65.} *Id.* Lena Rao, *Twitter Seeing 90 Million Tweets Per Day, 25 Percent Contain Links*, TECH CRUNCH (Sept.14, 2010), http://techcrunch.com/2010/09/14/twitter-seeing-90-million-tweets-per-day/.

^{66.} Payne, supra note 63, at 848.

^{67.} *Id.* at 841–42.

^{68.} Peter Vieth, Facebook 'Sideshow' No Distraction, Lawyer Says, VIRGINIA LAWYERS WEEKLY, Dec. 16, 2010. The defense in the case had sought to use pictures of the plaintiff "drinking a beer and having a his arm around a girl" to contest his claim for post-traumatic stress disorder after the death of his wife. After the plaintiff deleted the photos from his Facebook account despite receiving a discovery request for them, his lawyer was sanctioned in the amount of \$6,000 and the jury was twice instructed it could draw adverse inference from the destruction of this evidence. Nevertheless, the jury awarded plaintiff nearly \$10.6 million, one of the highest awards ever in Virginia death cases, which prompted plaintiff's lawyer to remark that the deleted pictures "didn't make a hill of beans."

 $^{69.\} Facebook\ Alibi\ Frees\ Brooklyn\ Man\ Rodney\ Bradford\ From\ Jail,\ CBS\ NEWS\ (Nov.\ 19,\ 2009),\ http://www.cbsnews.com/8301-504083_162-5675551-504083.html.$

Vol. 8:1

possession of third parties.⁷⁰

From emails and text messages, to online shopping and banking, the technology revolution has created the e-client. Since at least the 1990s, electronic evidence has been vital in determining the outcome of cases involving allegations of sexual harassment, disputes over trade secrets, copyright infringement, and insider trading. It's only a matter of time before litigation, and especially e-discovery, directly confronts the reality of cloud computing. As ESI increasingly shifts into the hands of third parties, such as social media networks, there is little doubt that it, and the metadata authenticating it, will continue to be relevant and potentially discoverable in a variety of litigation contexts. As third-party custodians of that information, cloud computing providers will likely play roles ranging from inadvertent spoliator to last-chance source of "smoking gun" evidence. Whether seeking information or complying with discovery expectations, all parties have a stake in minimizing and preventing loss or material alteration of data stored in the cloud.

III. THE PROBLEMS OF PRESERVATION

From business transactions to financial arrangements to social interactions, more than ninety percent of all information created and stored today is in the form of ESI.⁷⁴ Already eighty percent of all business records are never converted to paper.⁷⁵ "As businesses increasingly rely on electronic record keeping, the number of potential discoverable documents has skyrocketed and so also has the potential for discovery abuse."⁷⁶ "As documents are increasingly maintained electronically, it has become easier to delete or tamper with evidence (both intentionally and inadvertently) and more difficult for litigants to craft policies that ensure all relevant

^{70.} See PAUL R. RICE, ELECTRONIC EVIDENCE: LAW AND PRACTICE 185–86 (ABA 2nd ed. 2008) (Evidentiary value may exist only in a deviant or later version of a file stored in another location, and parties seeking to use ESI as evidence will have to address questions of the trustworthiness of the source). Not only is data created and stored through social networks discoverable evidence, attempts to delete it prompted a charge of evidence-tampering against a Rutgers University student whose alleged use of Twitter to promote an online video of a classmate led to the classmate's suicide. See Associated Press, Deleting Called Tampering With Evidence, TIMES UNION (Apr. 24, 2011, 12:01 a.m.), http://www.timesunion.com/news/article/Deleting-called-tampering-with-evidence-1350074.php.

^{71.} Kimura & Yamamoto, supra note 38, at 161.

^{72.} Redish, supra note 6, at 563.

^{73.} The Sedona Conference defines metadata as "information about a particular data set which describes how, when and by whom it was collected, created, accessed, or modified and how it is formatted." The Sedona Principles: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age THE SEDONA CONFERENCE, 94 (Sept. 2005), http://www.thesedonaconference.org/content/miscFiles/TSG9_05.pdf.

^{74.} Kimura & Yamamoto, supra note 38, at 154-55.

^{75.} Id. at 162.

^{76.} In re Seroquel Prod. Liab. Litig., 244 F.R.D. 650, 653-54 (M.D. Fla.).

documents are preserved."⁷⁷ But if courts are still coming to terms with just the proliferation of ESI, what will happen when all that information migrates into the hands of third parties?

E-discovery issues in the cloud computing paradigm will increasingly become centered on the complex relationship between the responding party, its inside and outside counsel, and one or more third-party custodians and vendors. A common issue, whether litigated or not, will be the implementation of litigation holds and effective preservation and production of data stored "in the cloud." Another will be the burden on counsel to fill the space between the client and the cloud service provider, and the extent of counsel's liability when spoliation occurs—in other words, the extent of the burden that will be placed on responding parties and their counsel to ensure ESI is produced from the cloud or, at least, that sanctions against them are not appropriate. Though perfect preservation is not even the goal, 79 how much data and potential evidence will simply be allowed to slip away because third parties do not have an enforceable prediscovery obligation to preserve?

A. THIRD-PARTY DUTIES ARE DISPROPORTIONATE TO THEIR ACTUAL CONTROL

As a part of routine discovery, a party may serve on any other party a request to produce certain items, including ESI, that are in the responding party's "possession, custody, or control." In the context of cloud computing, "control" is usually the most relevant test for the end user, since the service provider most likely has possession and custody. "Control" as used in Federal Rule of Civil Procedure 34 refers to the "right, authority, or practical ability to obtain" from a nonparty to the action. A number of cases have gone to significant lengths to make parties to the litigation responsible for ESI lost while in the possession of a third party if

^{77.} Zubulake v. UBS Warburg L.L.C., 220 F.R.D. 212, 214 (S.D.N.Y. 2003).

^{78.} Narkiewicz, *supra* note 22, at 56; *see also* Orbit One Communs., Inc. v. Numerex Corp., 271 F.R.D. 429, 436 (S.D.N.Y. 2010) (identifying the boundaries of the duty to preserve involve not just *when* the duty attaches and *what* evidence must be preserved, but "*how* must a party go about fulfilling its ultimate obligation, and *who* is responsible for seeing that it is fulfilled?") (emphasis in original).

^{79.} The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production, supra note 73, at no. 5.

^{80.} FED. R. CIV. P. 34(a).

^{81.} Venkat Rangan, *E-Discovery and the Cloud: Possession, Custody and Control*, E-DISCOVERY 2.0 (Sept. 3, 2010), http://www.clearwellsystems.com/e-discovery-blog/2010/09/03/e-discovery-and-the-cloud-possession-custody-and-control/.

^{82.} *In re* NTL, Inc. Sec. Litig., 244 F.R.D. 179, 195 (S.D.N.Y. 2007) ("*NTL*"); *see also* Moreno v. Autozone, Inc., No. C-05-4432 CRB, 2008 WL 906510, at *1 (N.D. Cal. Apr. 1, 2008) ("Control is generally defined as the legal right to obtain the documents on demand and at times has been construed more broadly to include the practical ability to obtain the documents sought upon demand.").

the information was at least nominally under the party's "control." To some extent, this practice has expanded the jurisdictional scope of the district court beyond its statutory 100 miles—courts have routinely extended the affirmative duty to preserve evidence far beyond its jurisdictional reach even where the evidence is not directly within the party's custody or control, so long as the party has access to, or indirect control over, such evidence. Does this still make sense in the cloud computing paradigm given the mutability of ESI and the limited ability of parties to actually control the preservation of data? Should it matter whether a third party has been entrusted with potential evidence only after it's been identified as such or whether it is the normal and customary "custodian" of such information? Circuits are split as to whether the practical ability to obtain materials is sufficient to constitute "control" in the meaning of Rule 34.

Of course, the fact that the information was stored on a third party server alone is not sufficient to challenge "control." For example, where a service provider destroys information because the party stops paying for its services and cancels its contract, any spoliation of evidence can appropriately be blamed on the party. But practically speaking, what a party can "access" is not necessarily the same as what the party can "control" —cloud computing and the Internet make access a much broader category than control. Who, for example, has control over the notes of an insurance adjuster entered on a handheld device from a car onto a remotely hosted word processing application? What may be merely accessed through a contractual or agency relationship but not controlled is vulnerable between the attachment of a duty to preserve and a formal request for discovery. So

Vol. 8:1

^{83.} See, e.g., In re Flag Telecom Holdings, Ltd. Sec. Litig., 236 F.R.D. 177, 180 (S.D.N.Y. 2006) ("The test for the production of documents is control, not location Documents may be within the control of the party even if they are located abroad."); see also, Victor Stanley, Inc. v. Creative Pipe, Inc., 269 F.R.D. 497, 523–24 (D. Md. 2010).

^{84.} See Victor Stanley, 269 F.R.D. at 523–24.

^{85.} Consider Facebook, for example. By creating an account, one gains "access" to a variety of information about other users with very little, if any, control over the content.

^{86.} *In re NTL, Inc. Sec. Litig.*, 244 F.R.D. at 195; Chaveriat v. Williams Pipe Line Co., 11 F.3d 1420, 1426–27 (7th Cir. 1993).

^{87.} See, e.g., Cyntegra, Inc. v. Idexx Lab., Inc., No. CV 06-4170 PSG, 2007 WL 5193736, at *5 (C.D. Cal Sept. 21, 2007).

^{88.} Thomas A. Cooper, *Jurisdictional, Procedural, and Economic Considerations for Non-Party Electronic Discovery*, 59 EMORY L.J. 1339, 1353 (2010).

^{89.} It may be, however, that the current broad reading of control can be narrowed on the back end by limiting what is "reasonably accessible," and therefore subject to production during discovery, to that which the responding party could have reasonably indentified and preserved given both the foreseeability of the issues in litigation and the relevant practical challenges. In fact, similar considerations are generally used to exempt metadata from the ordinary scope of the preservation duty. The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production, supra note 73, at nos. 5 and 9.

Winter 2012 THIRD PARTY PRESERVATION

While a third party may play a relatively large role in the actual preservation and maintenance of information on a daily basis in the course of its normal business practices, such a custodian who negligently or willfully destroys evidence in its possession faces little consequence, if any, apart from those it has contracted to sustain or which might be inflicted on its reputation in the market. Although parties to a lawsuit must accept the reality that discovery is by definition invasive and potentially very expensive, nonparties have a different set of expectations.⁹⁰ Third parties should not be required to subsidize litigation in which they do not have a stake, and they do not have a general duty to preserve evidence for use by others.⁹¹ A nonparty's responsibility to preserve information is generally limited to the mutual obligations of a contract or other agreement, 92 or an independent obligation under a statute or regulation, such as applies to auditors under the Sarbanes-Oxley Act of 2002, 93 stock exchanges, and securities dealers under the Securities and Exchange Act,⁹⁴ and various implementing regulations under the Fair Labor Standards Act.95 But violation of these statutory duties, even by a party, will not necessarily result in an award of sanctions in favor of a requesting party. 96 This reality is cold comfort to those situated like the plaintiff, for example, in the introductory hypothetical.

"[W]hen does the duty arise to preserve evidence or items that potentially could become evidence? To whom does this duty extend? And, what items must be preserved? Answers to these three questions are of critical importance for attorneys who counsel their clients." These questions are all the more important when the client has entrusted possession and custody of potential evidence to a third party, because under current federal rules and statutory regimes, the penalty for third party spoliation of evidence will always fall, if anywhere, on one of the parties. 98

205

^{90.} Cusumano v. Microsoft, 162 F.3d 708, 717 (1st Cir. 1998).

^{91.} Sedona Conference Commentary on Non-Party Production & Rule 45 Subpoenas, THE SEDONA CONFERENCE, 3 (Apr. 2008), available at http://www.thesedonaconference.org/dltForm?did=Rule_45_Subpoenas; Fletcher v. Dorchester Mut. Ins. Co., 773 N.E.2d 420, 424–25 (Mass. 2000).

^{92.} See generally Benjamin J. Vernia, Negligent Spoliation of Evidence, Interfering With Prospective Civil Action, as Actionable, 101 A.L.R 5TH 61, § 9 (Agreement).

^{93.} See 18 U.S.C. § 1520(a)(1)-(2) (2006).

^{94.} See 15 U.S.C. § 78q(a) (2006).

^{95.} See 29 U.S.C. $\$ 211(c) (2006); 29 C.F.R. $\$ 516.5-6 (2006).

^{96.} See, e.g., Sarmiento v. Montclair State Univ., 513 F. Supp. 2d 72, 94 (D.N.J. 2007) (adverse inference not available against defendant employer where its failure to preserve records was a violation of a federal statutory obligation because the litigation was not reasonably foreseeable at the time of the spoliation).

^{97.} MARGARET M. KOESEL & TRACEY L. TURNBULL, SPOLIATION OF EVIDENCE: SANCTIONS AND REMEDIES FOR DESTRUCTION OF EVIDENCE IN CIVIL LITIGATION 1 (ABA 2d ed. 2006).

^{98.} See KOESEL & TURNBULL, supra note 97, at 18–21 ("A duty to preserve may extend beyond the parties themselves and extend to evidence entrusted to their agents, experts, insurers, attorneys, and the like. In such instances, a party may be held liable for spoliation committed by a third party to whom it entrusted the destroyed evidence.").

B. Preservation tools are ineffective against third parties

The general lack of a duty to preserve is the basic flaw in using existing preservation tools to encourage a third party to take steps towards segregating and preserving potential evidence. As discussed below a party can pay for additional storage or other services, but it cannot expect the third-party vendor to assume any preservation responsibilities, apart from those to which it has contractually obligated itself, without additional compensation. One can put the vendor of one's opposing party on notice with a preservation letter, if their identity is known, but this does little, if anything, to shift the underlying responsibilities for preservation. Parties today cannot stop paying for cloud services and force their vendors to continue preserving their data pursuant to an independent legal duty to do so.

At the early stage of an initial litigation hold, potentially before litigation has even commenced, the burden of "freezing" the relevant data in the cloud could be overwhelming for the potential litigant, the third party, or both. The reliability of any computer system and the information gleaned from it can be a difficult issue when the servers are located just in the next room. But even when computer systems function perfectly, ESI remains fluid and dynamic and thus can be altered or destroyed by the ordinary operation of a computer, often without the operator's knowledge or direction.⁹⁹ Practices like multi-tenancy draw into question the feasibility of easily segregating and searching through the ESI of a particular user, with implications for determining which data is "reasonably accessible."100 In the cloud, the data fragmentation and dispersal that enhances security also creates a data retention challenge and a potential exposure to foreign laws. 101

At the same time, cloud computing will probably exponentially increase the amount of potentially discoverable "documents," as data about data becomes increasingly probative. The ability or willingness of a cloud computing service provider to produce information stored on its servers, may be limited by the Stored Communications Act ("SCA"). Because no cause of action lies against any provider for producing information, facilities, or assistance in accordance with the terms of a court order,

206

^{99.} Mia Mazza et al., *In Pursuit of FRCP 1: Creative Approaches to Cutting and Shifting the Costs of Discovery of Electronically Stored Information*, 13 RICH. J.L. & TECH. 11, 4 (2007). *See also* Kraus, *supra* note 6 ("disks corrode, bits "rot" and hardware becomes obsolete").

^{100.} The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production, supra note 73, at no. 8.

^{101.} Mell & Grance, supra note 27, at slides 22, 24.

^{102.} Stored Communications Act, 18 U.S.C. § 2701 (2006).

207

warrant, subpoena, or statutory authorization, ¹⁰³ cloud services providers typically require a court to mandate production of their customers' ESI without consent. ¹⁰⁴

But email and its protections under the current form of the SCA may prove to be an exception rather than the rule in the cloud computing paradigm, and perhaps rightly so. 105 Many cloud computing services arguably fail to qualify for the privacy protections of the SCA because they do not meet one or both of the statutory requirements of "electronic storage," which must be either of a temporary and intermediate nature, incidental to electronic transmission, or stored by the provider for the purpose of backup protection. 106 For example, some word processing applications merely allow for the sharing of data, rather than its communication—the data itself never leaves the providers cloud and thus the "send or receive" functionality required by the SCA is lacking. 107 Similarly, the authority to access users' data for a wide variety of purposes other than mere storage or processing, such as for generating targeted advertisements, takes many cloud computing service providers outside the current SCA definition of a "remote computing service." Thus, it may not be as easy in the future to simply assume that service providers are shielded by statute from producing any user content in their possession or custody. Though the SCA provides an important privacy safeguard for computing network users, particularly those on social networking sites and Web 2.0, it seems the primary civil litigation impact of cloud computing will be in the number of nonpersonal records entering the cloud that are less likely to involve privacy issues. 109 In other words, just because ESI is stored in the cloud doesn't mean it is necessarily "private" or should be subject to heightened procedural safeguards. As a result, third parties with relevant ESI in their cloud should be increasingly expected to produce from their servers. 110

^{103.} Stored Communications Act, 18 U.S.C. § 2703(e) (2006).

^{104.} See, e.g., Rangan, supra note 81.

^{105.} See Marcia Hofmann, Social Media Seeking User Data Share This, CALIFORNIA LAWYER (Mar. 2011).

^{106.} Robison, supra note 25, at 1209.

^{107.} Id. at n. 97.

^{108.} Id. at 1212-14.

^{109.} For example, in 2011 the U.S. Supreme Court determined that the privacy exemption to the Freedom of Information Act does not apply to the information of corporations. See F.C.C. v. AT&T Inc., 131 S. Ct. 1177, 1181 (2011). In the rare case that a third party subpoena seeks information that would constitute a trade secret, existing considerations regarding the use of protective orders would likely be sufficient.

^{110.} See Thomas Y. Allman, Conducting Discovery After the Amendments: The Second Wave, 10 SEDONA CONF. J. 215, 216 (2009) ("[R]elevant information in operating systems, dynamic databases, websites and voicemail ("digital audio files"), for example, can be discoverable whether found on individual or networked hard drives or on personal devices such as cell phones and PDAs.") (citations omitted).

If a court order is required, one approach to ensuring early preservation is to seek a preliminary injunction. An injunction entered under Rule 65 can bind the agents or servants of a party, and a court may use civil contempt sanctions to deter or punish third-party spoliation if preservation has been ordered by the court. However, the evidentiary showing necessary to obtain such a preliminary injunction or TRO makes this a cumbersome method for ensuring the preservation of data held by a third party prior to the ordinary discovery process when, presumably, the extent of the relevant information available first comes to light. ¹¹² In any event the pre-litigation duty to preserve is not enforceable against third parties in federal court under Rule 65—only an analogous duty can be imposed through an injunction when specific ESI can be identified for preservation against a manifest threat of destruction or deletion and a high likelihood of resulting prejudice. The extent of such a showing would likely have to approximate or exceed the cost of implementing the desired preservation unless the moving party voluntarily undertakes part of the cost. It remains to be seen if a party could meet this threshold to enjoin its own vendor to preserve evidence at the party's expense, but at the vendor's risk of contempt for spoliation. Increasing familiarity with cloud computing will shift standards of reasonableness over time, in terms of privacy expectations, accessibility and, potentially, culpability. 113 But even if customs develop to assume a quasi-duty to preserve on the part of third parties, judges will be hesitant if not stridently resistant to forcing any significant level of involuntary burden for preservation to a third party.

C. PRODUCTION TOOLS ARE INEFFECTIVE AT ENFORCING OR ENCOURAGING PRESERVATION

To the extent that third parties can be compelled to produce documents during discovery, procedures that do so are typically not

Vol. 8:1

^{111.} FED. R. CIV. P. 65(d)(2) (stating that "the order binds the parties, their officers, agents, servants, employees, and attorneys and other persons who are in active concert or participation with anyone described in Rule 65(d)(2)(A) or (B)").

^{112.} See Sierra Club, Lone Star Chapter v. F.D.I.C., 992 F.2d 545, 551 (5th Cir. 1993) (to obtain a preliminary injunction, a party must show that there is a substantial likelihood that it will succeed on the merits, that there is a substantial threat that it will suffer irreparable injury if the district court does not grant the injunction, that the threatened injury to the plaintiff outweighs the threatened injury to the defendant, and that granting the preliminary injunction will not disserve the public interest). CHARLES A. WRIGHT ET AL., FEDERAL PRACTICE & PROCEDURE § 2951 (2d ed. 2011) ("When the opposing party actually receives notice of the application for a restraining order, the procedure that is followed does not differ functionally from that on an application for a preliminary injunction and the proceeding is not subject to any special requirements.") Any temporary restraining order granted without notice must comply with the provisions of Rule 65(b).

^{113.} See, e.g., City of Ontario v. Quon, 130 S. Ct. 2619, 2929 (2010) ("Rapid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior.").

effective means of ensuring preservation. A Rule 45 subpoena can be used to compel production of ESI, and is in fact usually required for the production of emails from third parties. Amendments made to Rule 45 in 2006 were intended to explicitly recognize the existing practice of seeking Rule 45 subpoenas for such requests. The issuance of a subpoena to a third party imposes a legal obligation on the third party to preserve information relevant to the subpoena, including ESI, at least until related issues are resolved. In some circumstances, the subpoena itself could make the recipient a potential party in foreseeable litigation, but service of and compliance with a nonparty subpoena alone is generally not sufficient to create an independent duty to preserve.

Many of the 2006 amendments to Rule 45 were simply borrowed language from Rules 26 and 34 with appropriate wording to clarify its applicability to subpoenas. 118 This fact reflects the general approach to nonparty production taken by the Sedona Conference and rule-makers that it is essentially the same as production from parties. Naturally, the consequences for spoliation after the issuance of an injunction or a subpoena include the full range of penalties available for contempt of court including, in extraordinary cases, imprisonment. 119 But as with injunctions under Rule 65, subpoenas under Rule 45 suffer the basic flaw that they do not impose an obligation on a third party to preserve ESI or other evidence until after a lawsuit has been initiated, which can often be a considerable time after the duty to preserve has attached to the responding party. 120 Where subpoenaed evidence is not available due to spoliation, the question before the court is generally whether the third party complied with the terms of the subpoena, not whether the party properly preserved evidence prior to its issuance. 121 If it can be shown that the data was already lost prior to its issuance, the subpoena is of no consequence. In the meantime, the responding party or its counsel bear the sole burden of ensuring preservation of ESI in the cloud with little means of actually doing so. 122

^{114.} See generally Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965 (C.D. Cal. 2010).

^{115.} Sedona Conference Commentary on Non-Party Production & Rule 45 Subpoenas, supra note 91, at 3.

^{116.} Id.

^{117.} Id.

^{118.} Id.

^{119.} See Victor Stanley, Inc. v. Creative Pipe, Inc., 269 F.R.D. 497, 537 (D.Md. 2010).

^{120.} See, e.g., In re Cree, Inc. Sec. Litig., 220 F.R.D. 443, 447 (M.D.N.C. 2004) (preservation subpoena served without leave of court quashed despite risk that routine document destruction policy might destroy relevant evidence).

^{121.} Rimkus Consulting Group, Inc. v. Cammarata, 688 F. Supp. 2d 598, 607 (2010).

^{122.} To get around the restrictions of the SCA, a federal magistrate in the Middle District of Tennessee proposed the parties "friend" him on Facebook, thus providing mutual access to disputed photos and emails. See Terry Baynes, Should You Friend the Judge?; Social media presents a new front for discovery battles, THE AMERICAN LAWYER, Sept. 1, 2010, http://www.law.com/jsp/tal/PubArticleTAL.jsp?id=1202472760856&slreturn=1.

As a result any penalties against the non-party for contempt, even if remedial in some cases, are an ineffective incentive for pre-litigation preservation. Perhaps more importantly, injustice to an actual litigant is a likely result whenever the requesting party is substantively prejudiced by the unsanctioned loss of crucial evidence, or if a sanctioned party is simply a stand-in for the third party and thereby itself becomes the victim of negligent or willful spoliation. 124

The use of production methods to preserve and obtain information from the cloud is further complicated by the fact that data may be difficult to separate from confidential or proprietary information of the party, the vendor, or other third parties. Though a party generally does not have standing to challenge a nonparty subpoena, a party whose information is sought can move to quash under the SCA as to its own privacy interests. ¹²⁵ Courts seem willing and able to protect messages that are inherently private while distinguishing and protecting those that are not, ¹²⁶ notwithstanding the general rule that any person who does not provide an electronic communication service, or a remote communication service, can "disclose or use with impunity the contents of an electronic communication unlawfully obtained from electronic storage. ¹²⁷

The third party can likewise move to quash or modify a subpoena to protect privacy interests.¹²⁸ For example, information about how a party uses a cloud-based platform might only be derivable through information residing exclusively in the data structures or processes of the cloud not set out in any particular data output available to the user.¹²⁹ The vendor may in

^{123.} Consider, for example, the plight of Monica Lips, whose products liability case against the manufacturer of her defective hip replacement suffered an initial setback when the hospital that removed the prosthesis from her body destroyed the pieces. Lips' claim against the hospital was dismissed and the decision was affirmed by the Arizona Supreme Court, which decided not to recognize an independent tort for intentional spoliation. Lips v. Scottsdale Healthcare Corp., 229 P.3d 1008, 1009 (Ariz. 2010); see also Pat Murphy, Arizona Supreme Court: Is hospital liable for losing key evidence?, LAWYERS USA, May 10, 2010, http://lawyersusaonline.com/benchmarks/2010/05/10/is-hospital-liable-for-losing-key-evidence/. The court declined to comment on the viability of a negligent spoliation tor in the state since Lips had only alleged intentional spoliation on the basis that her surgeon had requested the preservation of the prosthesis. It remained to be seen what effect the decision would have on the underlying suit against the manufacturer, but the spoliation claim alleged that the underlying suit was compromised by the destruction of crucial evidence.

^{124.} See Keir v. Unumprovident Corp., No. 02 Civ. 8781, 2003 WL 21997747 at *13 (S.D.N.Y. Aug. 22, 2003) (defendant sanctioned for accidental spoliation of emails by third-party vendor).

^{125.} See Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 973–76 (C.D. Cal. 2010).

^{126.} For example, in *Crispin*, the court quashed a subpoena as to Facebook and MySpace postings filtered so they could only be viewed by "friends" rather than the general public, while remanding for development of the record as to whether wall posting and comments would be similarly protected from discovery. *Id.* The private messages were likened to videos not marked for public access in Viacom Int'l Inc. v. YouTube Inc., 253 F.R.D. 256 (S.D.N.Y. 2008).

^{127.} Crispin, 717 F. Supp. 2d at 973 (quoting Wesley College v. Pitts, 974 F. Supp. 375, 389 (D. Del.1997)).

^{128.} See FED. R. CIV. P. 45(c)(3)(A)(iii), (d)(2).

^{129.} Chris Reed, Information "Ownership" in the Cloud, QUEEN MARY SCHOOL OF LAW LEGAL

fact have proprietary interests, or even copyright, in creatively structured databases. ¹³⁰ Even identifying the correct vendor may be challenging if a cloud provider incorporates proprietary services of other companies as part of its own service or allows other companies to use its platform to provide services directly to the end user. ¹³¹ Though spoliation is not the primary concern in such instances, the confidentiality concerns that can attend production of proprietary information make the use of subpoenas to reveal flaws in preservation unwieldy at best.

IV. PRESERVATION PROPHYLAXIS

Rule makers are still undecided whether a new preservation rule is necessary, let alone what form it would take. While consideration of the topic provides a useful opportunity to examine how control and accessibility of data in the cloud shape the application of proportionality to preservation, the answers to the types of questions posed earlier by the introductory hypothetical depend in the meantime on the contract between the insurer and its cloud service provider. Cloud computing is a service industry, and therefore, the businesses in this space are constantly under pressure to modify their offerings to the perceived needs of the market. Given that a third party's obligations to preserve data on their servers is generally limited to their terms of service agreements, these agreements are a natural place to start when looking for peace of mind at in the cloud. With the exception of a relatively few niche service providers, however, contracting for data integrity may come at the cost of some of the features that attract businesses to cloud computing in the first instance.

A. TERMS OF SERVICE AND THE COST OF "PEACE OF MIND"

As a starting point, most cloud service providers expressly disclaim liability for lost data.¹³⁴ Some promise "best efforts" to preserve data, but assert a general disclaimer and keep on the end user the responsibility for

STUDIES RESEARCH PAPER No. 45/2010 1, 8 (2010), http://papers.ssrn.com/sol3/papers.cfm? abstract_id=1562461.

^{130.} Reed, supra note 129, at 15 (citing Feist Publications, Inc. v. Rural Telephone Services Co., Inc., 499 U.S. 340 (1991)).

^{131.} Id. at 5-6.

^{132.} Agenda for April 2011 Meeting, supra note 29, at 194.

^{133.} Rackspace, a data backup service, advertises on their website that their solutions "deliver nothing less than peace of mind." *Unmetered Managed Backup*, RACKSPACE HOSTING, http://www.rackspace.com/managed_hosting/services/storage/managedbackup (last visited July 31, 2011).

^{134.} Simon Bradshaw, Christopher Millard, & Ian Walden, Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services, QUEEN MARY SCHOOL OF LAW LEGAL STUDIES RESEARCH PAPER No. 63/2010 1, 21–22 (2010), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1662374.

preserving the confidentiality and integrity of its own data.¹³⁵ The disclaimers of most vendors make clear that there is no warranty as to the quality or fitness of their service for any particular purpose.¹³⁶ From here, many service providers provide further guarantees if the end user agrees to purchase separate backup services.¹³⁷ Others provide data backup and integrity services without additional charge, but also without any express guarantee of preservation.¹³⁸ Few take any effort to ensure that data is stored in any particular location or jurisdiction, though some have servers configured in regional zones in which data can be corralled with predictability.¹³⁹

If standard backup packages are not enough to provide satisfaction about one's remotely stored data, another option is to negotiate a bespoke contract with a variety of additional guarantees and indemnifications. ¹⁴⁰ If, for example, the hypothetical insurer had gone to this length, it might have the option of either settling the case with the homeowner on the basis of monies paid by the provider or litigating with the knowledge that some form of indemnification or contribution could be available. But relying on this sort of feature of a terms of service agreement in cases involving significantly larger claims than a single homeowner's insurance policy would likely be problematic; custom arrangements can include liquidated damages clauses for the relatively predictable business consequences of data loss or disclosure of proprietary information, but will likely not extend to court ordered sanctions for spoliation or failure to comply with an order In any event, most terms of service agreements have limitations on liability ranging from the amount paid for a single month of service to a multiple of the total amount paid for service to date. ¹⁴¹ Another challenge might be learning of a claim in time to bring it under a terms of service agreement that contains a limitation period of two years or less. 142 The process of getting the vendor "on the hook" for the preservation of data appears to be as much about providing peace of mind for the vendor as for its customer.

At least one popular provider of premium preservation services offers managed backup on a daily, weekly, or incremental basis to physical media such as tapes or discs.¹⁴³ Far from some technological innovation, this service is essentially identical to the types of backups businesses have been

^{135.} Bradshaw, et al., *supra* note 34, at 21–22.

^{136.} Id. at 32–33.

^{137.} Id. at 22.

^{138.} *Id*.

^{139.} Id. at 27-28.

^{140.} Id. at 2.

^{141.} *Id.* at 36.

^{142.} Id. at 18.

^{143.} Rackspace Managed Backup: Technical Overview, RACKSPACE HOSTING, (2009), http://broadcast.rackspace.com/downloads/pdfs/ManagedBackupTechOverview.pdf.

making in-house for decades, and suffers the same restoration challenges. The difference is that once computing infrastructure itself has been outsourced, backup and preservation must follow. Unless there are significant scalability issues, wildly variant peak and trough usage periods, or a profound need for remote access, it becomes less clear whether outsourcing the company's entire information technology department actually provides the risk-adjusted benefits originally perceived. This realization is particularly acute for large concerns that are subject to frequent litigation and exist under virtually perpetual threat of foreseeable litigation.

Thus, the final and, ultimately, only way to tailor the terms of service to offset the risks of preservation in the cloud is to limit use. Mature companies with more predictable information flows and computing needs may prefer to retain much of their information technology infrastructure inhouse or to maintain private clouds with outsourced support. Such companies might use public cloud resources for limited categories of data only, focusing on those that require little access (essentially leasing storage space) or those that benefit most from shared access, such as early-stage development projects. Limiting the potential types of data losses to those that are best compensated by liquidated damages clauses likely provides the mix of scalability, flexibility, integrity, and security that most closely approximates actual peace of mind.

B. NEW RULES

Since the 2010 Civil Litigation Conference at Duke University, the Advisory Committee on Civil Rules has taken a serious look at further amending the Federal Rules with respect to discovery. Though agreement on the need for such a rule has not been completely unanimous, the general consensus seems to be that the principle of proportionality that now governs the scope of production should also be incorporated into considerations of preservation. It is beyond the scope of the current work to discuss the methods by which this might occur other than to briefly discuss some of the potential implications in the cloud computing paradigm and to suggest that a practical understanding of access to and control of data in the cloud should be the foundation of any normative framework for proportionality in preservation.

A preservation standard incorporated into the Federal Rules would likely emphasize reasonableness and proportionality as essential contours of the duty to preserve.¹⁴⁵ "Whether preservation or discovery conduct is acceptable in a given case depends on what is *reasonable*, which itself

^{144.} Agenda for April 2011 Meeting, supra note 29, at 194.

^{145.} Allman, supra note 30, at 145.

depends on whether the requested discovery efforts are *proportional* to the case and consistent with established standards."¹⁴⁶ In other words, the duty to preserve will always be determined by an analysis that "depends heavily on the facts and circumstances of each case and cannot be reduced to a generalized checklist of what is acceptable or unacceptable."¹⁴⁷ In the context of this amorphous obligation on courts, parties, and counsel, a practical understanding of control and accessibility in the cloud computing paradigm has a profound potential for creating some level of objectivity and predictability in preservation and e-discovery.

One of the most attractive features of cloud computing to business users is its scalability, which refers to the ability to purchase only as much or as little storage, processing and bandwidth as needed at any given time. The pay-per-use model allows users to limit their costs to the amount of storage and bandwidth actually used. But this model turns against a party seeking to implement a litigation hold with respect to data in the cloud to the extent doing so would require the purchase and use of extra bandwidth, processing, or storage to identify, collect, and preserve data related to foreseeable litigation. Unlike the restoration of backup tapes, which only becomes an issue with respect to production, the cost of exercising control over data in the cloud would likely result in significant costs at the initial preservation stages, cost which might someday replace the restoration of backups as the main object of discovery cost-shifting disputes. Given that the cloud computing paradigm encourages users to maintain relatively little onsite storage capacity, even the theoretical ability to re-route ESI may not necessarily translate into actual control of the data or a practical ability to do so. 148

Even where parties carefully manage their information, it's not clear that cloud computing users necessarily have ready access to all potentially relevant information, particularly metadata. The general rule is that there is no duty to preserve material on inaccessible media, ¹⁴⁹ and metadata is presumptively inaccessible unless there is a particular showing of relevance. Where the issue is one of authentication or creating a timeline

Vol. 8:1

^{146.} Allman, *supra* note 30, at 145 (quoting Rimkus Consulting Group, Inc. v. Cammarata, 688 F. Supp. 2d 598, 613 (2010) (emphasis in original)).

^{147.} Rimkus, 688 F. Supp. 2d at 613 (citing Pension Comm. of Univ. of Montreal Pension Plan v. Banc of Am. Sec., 685 F. Supp. 2d 456, 464–65 (S.D.N.Y. 2010)).

^{148.} See Columbia Pictures, Inc. v. Bunnell, 245 F.R.D. 443, 453 (C.D. Cal. 2007) ("data in issue which is currently routed to a third party entity under contract to defendants and received in said entity's RAM . . . is within defendants' possession, custody or control by virtue of defendants' ability to manipulate at will how the data in issue is routed").

^{149.} Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 217 (S.D.N.Y. 2003) ("Must a corporation, upon recognizing the threat of litigation, preserve every shred of paper, every e-mail or electronic document, and every backup tape? The answer is clearly, 'no'. Such a rule would cripple large corporations."). The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production, supra note 73, at no. 8.

of access to a particular file, metadata will clearly be important and, therefore, should be within the scope of production. Increasingly, metadata will typically be in the category of information generated inside the cloud, the ownership of which is potentially subject to dispute. A showing of special need and relevance by a requesting party says nothing about the practical ability of a party to produce metadata in a meaningful form or the foreseeability of its eventual need to do so from within the pre-litigation context. Nevertheless, a narrow "front end" preservation rule is less likely to consistently produce just results than a broad "back end" rule that gives judges the discretion to tailor sanctions based on the centrality or importance of the evidence sought by the requesting party and the apparent culpability of the responding party. 151

It's also not clear that the distinction between active data and disaster backup is a particularly effective distinction for evaluating accessibility in the cloud computing paradigm. The approach to accessibility articulated by Judge Scheindlin in *Zubulake IV* defines certain formats of digital media, like backup tapes, as *per se* inaccessible. A party need not provide discovery of electronically stored information from sources that the party identifies as not *reasonably accessible* because of undue burden or cost. But even inaccessible data sources must be preserved if they store documents of key players to the existing litigation or where the responding party can identify where on the inaccessible sources the relevant information is stored. The principle of proportionality is then used to determine whether the likely probity of the information justifies the cost of production.

But while this *per se* distinction is explicitly predicated on concerns related to cost, it actually becomes unmoored from cost when the burden of

^{150.} Reed, supra note 129, at 8-9.

^{151.} See Agenda for April 2011 Meeting, supra note 29, at 194–95. For example, where the missing evidence is so important as to make it eminently foreseeable that it would have to be preserved for production, failure to do so—or arrange to do so with a service provider—should be sanctionable even though the actual destruction, loss, or modification of the evidence might not be intentional. On the other hand, where missing data would not have been particularly identifiable for its importance prior to a discovery request, there should be less inclination to impose sanctions on the same negligent action or inaction.

^{152.} The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production, supra note 73, at no. 5.

^{153.} Zubulake, 220 F.R.D. at 217–18 (S.D.N.Y. 2003).

^{154.} FED. R. CIV. P. 26(b)(2)(B) (emphasis added).

^{155. &}quot;Relevant information need not be admissible at the trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence." FED. R. CIV. P. 26(b)(1). For purposes of admissibility "'[r]elevant evidence' means evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence." FED. R. EVID. 401.

^{156.} Zubulake, 220 F.R.D. at 218 (S.D.N.Y. 2003). See also FED. R. CIV. P. 26(b)(2)(B) (identification of a source by a party as "not reasonably accessible does not relieve the party of its common-law or statutory duties to preserve evidence").

Vol. 8:1

preservation or production is due to a large volume of responsive data existing amongst many remote sources of otherwise reasonably accessible data. If, for example, data is located on "accessible" active media, but dispersed over several servers in multiple states or countries without a readily available means of downloading and segregating it, the cost of preserving and producing this information could exceed that of restoring backup tapes, and present all the same burdens, but would be required because the information is not per se inaccessible. 157 This is precisely the challenge many responding parties would likely face in the cloud computing paradigm. Unless the end user is proactively limiting the categories of data placed in the cloud as suggested above, 158 it is not clear that ESI stored in the cloud can be easily distinguished as that which is purely disaster recovery and that which is actively used for information retrieval—almost all data in the cloud is accessible to some degree. As a result, the practical burden of a reasonable, good faith preservation effort in the cloud seems unbounded by existing concerns of burden and cost unless proportionality is understood in terms of the types of accessibility and

It may be possible in some cases to shift the cost of preservation to the requesting party, as already occurs when necessary with regard to production and in the context of a Rule 45 subpoena, when preservation or production would impose an undue burden or expense on a nonparty. Conversely, where negligence on the part of the third party generates cost burdens in collecting, processing or producing, it should be possible to shift the cost away from the parties altogether in pursuit of the underlying facts. Otherwise, the existing incentive to keep in an accessible format only that

control available, and the cost thereof, in the third party paradigm. 159

^{157.} The obvious solution to such a problem, however, would be to limit the scope of the discovery request pursuant to Rule 26(b)(2)(C). After discovery of the most likely relevant and probative information, the scope could broaden until the responding party was able to make a credible showing that any further production would be duplicative or cumulative.

^{158.} See supra Section IV.A.

^{159.} On a motion to compel production, an opposing party may assert undue burden, for which it must demonstrate that the time or expense involved in responding to requested discovery is unduly burdensome. See, e.g., Oxford House, Inc. v. City of Topeka, Kansas, No. 06-4004-RDR, 2007 WL 1246200, at *4 (D. Kan. Apr. 27, 2007). But the mere fact that compliance will cause great labor and expense or even considerable hardship and the possibility of injury to the business of the responding party will not necessarily require denial of the motion, particularly if the information sought is highly relevant. Id. Though spoliation sanctions will not issue where a party cannot be compelled to produce lost ESI, at the preservation stage, the burden of determining where relevant material is stored is only examined under the rubric of "accessibility."

^{160.} See, e.g., Fendi Adele S.R.L. v. Filene's Basement, Inc., No. 06 CIV. 244RMBMHD, 2009 WL 855955, at *4 (S.D.N.Y. Mar. 24, 2009) (dispute over accessibility of backup tapes resolved by ordering production of electronic copies of backup databases at requesting party's expense).

^{161.} See, e.g., Dow Chem. Co. v. Reinhard, No. M8-85(HB), 2008 WL 1968302, at *2 (S.D.N.Y. April 29, 2008) (ongoing costs of attorneys' fees, privilege logs and other expenses assumed by complying with subpoenas to be shared between the subpoenaed party and the requesting party).

which is absolutely necessary for business purposes, ¹⁶² will serve as a disincentive to adoption of the cloud computing paradigm. Similarly, a *per se* rule for reasonably accessible data that excludes that stored in the cloud risks encouraging more frequent reduction to inaccessible formats where possible. ¹⁶³ In either case, the result would be the vast reduction of discoverable information or, at least, a significantly heavier burden on requesting parties.

Another approach is to encourage the parties themselves to stipulate what media will be considered reasonably accessible or inaccessible. 164 Though it is not clear how often this tactic is already used, and it might only prove useful in symmetric cases where the potential costs of discovery are roughly equivalent, district court judges are likely to embrace such an approach, particularly in light of the explicit "meet and confer" requirements of the federal rules and the frequent exhortation that parties should conduct e-discovery in the spirit of cooperation. 165 Allowing the parties to determine as early as possible what is or is not reasonably accessible allows for better calibration based on the likely relevance of various media and allows the parties to create a hierarchy of relevant, costeffective media from which responsive documents can be culled. And the effect is achieved without the creation of a "one size fits all" front-end rule that establishes a narrow framework for preservation obligations. The values served by stipulation are already emphasized under the existing Rule 16, but the benefits of this approach might justify further clarification and codification in the rules or committee notes.

V. CONCLUSION

The cloud computing paradigm appears poised to create a future in which the custodians of ESI are frequently nonparties for whom the duty to preserve as currently conceived does not effectively attach. To the extent that data in the cloud is more fluid, more challenging to authenticate, and potentially exists as bits scattered in servers around the world, traditional

^{162.} See, e.g., Best Buy Stores, L.P. v. Developers Diversified Realty Corp., 247 F.R.D. 567, 569–70 (D. Minn. 2007) (database produced for separate litigation not reasonably accessible because of a downgrade in format).

^{163.} One solution would be to simply require a responding party to transfer any data subject to a litigation hold to on-site servers or other local media, but this obligation would tend to undercut the benefits of cloud computing for any large companies that frequently find themselves in litigation. It would also create significant costs that might not be relevant to the court's determination of whether the data was "accessible."

^{164.} See, e.g., Agreed E-Discovery Protocol and Order at \P 7, Interval Licensing LLC v. AOL, Inc., (No. 2:10-CV-01385-MJP) 2011.

^{165.} See, e.g., Nat'l Day Laborer Org. Network v. U.S. Immigration and Customs Enforcement Agency, No. 10 Civ. 3488(SAS), 2010 WL 381625, at *8 (S.D.N.Y. Feb. 7, 2011) (the words "meet and confer," "cooperate," and "communicate" are found in opinion after opinion and yet lawyers fail to take the necessary steps to fulfill their obligations to each other and to the court).

notions of preservation do not apply neatly to the cloud computing paradigm. Because discovery sanctions are intensely fact-dependent and somewhat unpredictable, all stakeholders in litigation have an interest in minimizing the disruptive potential of third party custody of relevant information.

For a variety of reasons, the concerns expressed in this note may not ultimately motivate a significant departure from current practices. Cloud computing might not become as ubiquitous as currently expected, or technology may improve to the point where loss of evidence is no longer a significant issue. Service providers and their users may agree to terms of service that largely resolve these issues by better allocating the responsibility and cost of preserving data in the cloud in relation to the actual ability to do so. The diligence of ethics committees, bar associations and similar organizations may establish clear expectations that afford courts and attorneys sufficient confidence to navigate these issues with only modest difficulty. Or Congress could shift expectations by amending the SCA or other statutes that currently only create a preservation obligation for parties, such as the Private Securities Litigation Reform Act. 166

But if preservation rulemaking is contemplated, the potential benefits of including third-party custodians in the calculus should be considered. From the costs to businesses in terms of sanctions or settlement, to the effect on the cloud computing model and the ability of service providers to pass those costs on to their users, the practical ramifications of cloud computing on e-discovery today is no longer an academic question. The implications are staggering given the current approach to third-party spoliation. The handwriting is no longer just on the wall—it is stored in thousands of servers in multiple jurisdictions spread across the globe.

Businesses considering adoption of cloud services should weigh the potential implication for litigation preservation and production, and seek solutions from competent vendors that meet these long-view expectations. Judges and rule makers should look realistically at access to and control of data in the cloud when identifying active, reasonably accessible media and incorporating proportionality into their expectations for preservation. Lawmakers should consider whether the business of storing data should include an obligation to preserve evidence for litigation. In all cases, the goal should be to find ways of shifting the burdens of preservation to where

Vol. 8:1

^{166.} See Mark A. Berman and Aaron E. Zerykier, Preservation of Electronic Information by Nonparties under the Private Securities Litigation Reform Act, 16 SEC. LITIG. J. 10, 10 (2006), http://web2.customwebexpress.com/ganshore/UserFiles/File/PreservationOfElectronicInfo.pdf (ensuring preservation by nonparties during discovery stay under PSLRA requires preservation subpoena, for which a party first must seek relief from the court of the automatic stay by requesting "particularized discovery" and showing that such discovery is necessary either to preserve evidence or to prevent undue prejudice to that party).

Winter 2012 THIRD PARTY PRESERVATION

they are most appropriate and most easily borne rather than simply reducing expectations and undermining the litigation process.

219

220 HASTINGS BUSINESS LAW JOURNAL

Vol. 8:1

* * *

Share 0 More Next Blog» Create Blog Sign In



TUESDAY, NOVEMBER 15, 2011

Digital Library Federation Fall Forum 2011

I had the honor of attending this year's $Digital\ Library\ Federation\ Fall\ Forum\ a$ few weeks ago as a Forum Fellow and I wanted to share a little of my experience on the blog.

First of all, I am so grateful to the DLF for giving me the opportunity to attend. There were three fellows this year and each of us was paired with a mentor for the conference, which was fantastic. My mentor introduced me to a bunch of people and gave me some excellent advice about career planning and working in the field. It was also great to meet the other fellows and learn more about their experiences and paths into digital librarianship.

In addition to all the professional socializing inherently involved in conference attendance, I attended several really great presentations and workshops, but for the sake of brevity I'll just highlight a few:

UDFR: A Semantic Registry for Format Representation Information

This brief but informative session gave an update on the development of UDFR, the Unified Digital Format Registry. This registry will combine the existing PRONOM and GDFR registries to give a comprehensive, interactive listing of file formats, along with their significant properties and preservation risks. I can't wait to see the result, which should go live in early 2012.

Digital Preservation Cloud Services for Libraries and Archives

This session outlined some of the ways in which cloud services could be a solution for ongoing digital preservation needs among library and archive institutions. Cloud-based services can answer some common technological needs, including:

- Scalability cloud services allow for quick resource provisioning and are generally pay-as-you go.
- Cost-efficient maintenance cloud services can maximize resource use thanks to economy of scale.
- Configurability levels of service can be defined according to institutional policies and need.

However, there are still issues relating to cloud services, particularly in terms of reliability and security. I actually heard someone in a different session mention that they had lost data during transfer to and from a cloud storage provider, so...keep that in mind if you're considering cloud storage as a primary preservation solution. (Also keep in mind that this was just one person at one institution. Many other cloud service users may have had excellent experiences. Please share if you know of research in this area!)

Strategies for Film and Video Digitization

This 3-hour working session covered so much information that I have pages and pages of notes, so I'll just mention the topics that were discussed:

- Media preservation plans their importance, and an example from Indiana University
- File formats and digitization specifications
- Digitization as a preservation strategy this was really interesting, with examples of current practice from Northwestern, Indiana, and Stanford Universities
- Storage methods
- Workflow issues

A Google Doc with detailed notes from this session can be viewed here if you'd like to see more detail.

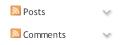
I also attended the post-forum Project Managers Meeting, in which I learned a lot about project

ABOUT US

Preservation Services is responsible for preserving the entire Dartmouth College Library collection to make it accessible for current and future students, faculty, and scholars. The Book Arts Program is also part of Preservation Services.

For more information about what we do, visit our web page.

SUBSCRIBE TO



LINKS

- Preservation Services Home
- Dartmouth College Library
- Rauner Library Blog
- AIC (American Institute for Conservation) Blog
- GBW (Guild of Bookworkers)
 Blog
- IUL Preservation Lab Blog
- Jeff Peachey
- Library Preservation 2
- Media Preservation (IU Bloomington)
- Parks Library Preservation (lowa State)
- PCAN (Preservation and Conservation Administration News)
- Preservation (UCLA Library)
- Preservation Beat (UI Libraries)
- The Signal: Digital Preservation (Library of Congress)
- TSLAC (Conservation at Texas State Library and Archives Commission)

LABELS

management practices. In addition to some excellent discussion, the highlight of this meeting for me was Tito Sierra's presentation on the Project One-Pager. His slides from that presentation can be found here, and I highly recommend looking them over if you're interested in project management.

All in all, the forum was fun and informative, and I'm really glad I was able to attend. Thanks, DLF!

Written by Helen Bailey

Posted by Preservation Services at 8:00 AM

Recommend this on Google

Labels: conferences, digital preservation

No comments:

Post a Comment

Enter your comment	
Comment as: Google Account ▼	
Publish Preview	
Newer Post	Home

Subscribe to: Post Comments (Atom)

- administrative
- assessment
- book arts
- Book Arts Prize
- Book Arts Program
- book repair
- chemistry
- circulating collections
- commercial binding
- conferences
- conservation
- Dartmouth happenings
- deacidification
- digital curation
- digital preservation
- digital production
- disaster response
- documentation
- events
- exhibits
- experiments
- film preservation
- Friends of the Library
- guests
- housing
- interns
- media preservation
- paper treatments
- papyrus
- personnel
- pointers
- policy

Older Post

- position vacancy
- Preservation Week
- preserving personal collections
- Readex
- resources
- special collections
- Special Instructor
- students
- tools
- training

SEARCH THIS BLOG



BLOG ARCHIVE

- **▶ 2012** (42)
- **2011** (70)
 - ▶ December (4)
 - ▼ November (5)

Association of Moving Image Archivists Conference

Guest Post from Intern Arini Esary

Digital Library Federation Fall Forum 2011 Visit from Professor Anna

Embree

Dartmouth College

Library Digital

Preservation Pol...

- October (8)
- ► September (8)
- August (6)
- ▶ July (4)
- ▶ June (5)
- ► May (6)
- ► April (8)
- ► March (8)
- ► February (7)
- ▶ January (1)
- **2010** (17)

CONTRIBUTORS



Helen K. Bailey
Is a graduate of the University
of Texas School of Information
with a Master of Science and
Information Studies (MSIS) and
a Certificate of Advanced
Study (CAS) in Library and
Archives Conservation. She is
currently a Preservation
Specialist responsible for
preserving Dartmouth College
Library's digital collections, as
well as a bookbinding
instructor in the Book Arts
Program.



Deborah Howe
Is the Collections Conservator
at Dartmouth College Library.
She's been involved in the
book community for over 20
years. She is a member of the
Guild of Book Workers and
teaches classes in the Book
Arts program.

Ryland lanelli

Is a cartoonist and Project Specialist in the Dartmouth Preservation Services department. He graduated from Reed College with a BA in Art History in 2008 and, more recently, from the Center for Cartoon Studies with an MFA in Cartooning in 2010. In addition to his work in Preservation and the Digital Production Unit, he is currently drawing and writing for various independently published comics and anthologies.



Is a Project Specialist and Book Arts instructor in the Preservation Services Department. After receiving a BA in Studio Art from Washington College (MD), she pursued a growing passion for bookbinding at the North Bennet Street School and earned a Diploma in Bookbinding in 2008. Along with managing her own bookbinding studio in Shelburne, VT, Elizabeth is the Chair of the Book Arts Guild of Vermont and a member of the Guild of Book Workers.



Barb Sagraves Barb has been head of Preservation Services since its creation in 1995. She is a graduate of the University of Michigan SLIS program, has an MA in Medieval History from Michigan State University, and a BA in History from the University of Oklahoma. In her role as department head, Barb has overall responsibility for the preservation program and policies at Dartmouth College Library and is in charge of the Book Arts Program.

Stephanie Wolff is a
Conservation Technician and
Book Arts Instructor at the
Dartmouth College Library.
Her Master of Arts in Liberal
Studies (MALS) degree from
Dartmouth College focused on
the book, including its
historical, cultural, and
artistic aspects. She shows
her artist's books in
exhibitions around the
country.

FOLLOWERS



Members (15)



Already a member? Sign in

Simple template. Powered by Blogger.

Trademark/Service Mark Application, Principal Register

Serial Number: 77922469 Filing Date: 01/28/2010

The table below presents the data as entered.

Input Field	Entered	
SERIAL NUMBER	77922469	
MARK INFORMATION		
*MARK	PRESERVATION CLOUD	
STANDARD CHARACTERS	YES	
USPTO-GENERATED IMAGE	YES	
LITERAL ELEMENT	PRESERVATION CLOUD	
MARK STATEMENT	The mark consists of standard characters, without claim to any particular font, style, size, or color.	
REGISTER	Principal	
APPLICANT INFORMATION		
*OWNER OF MARK	NextPoint Inc.	
*STREET	4043 North Ravenswood Ave., Suite 317	
*CITY	Chicago	
*STATE (Required for U.S. applicants)	Illinois	
*COUNTRY	United States	
*ZIP/POSTAL CODE (Required for U.S. applicants only)	60613	
LEGAL ENTITY INFORMATION		
ТУРЕ	corporation	
STATE/COUNTRY OF INCORPORATION	Illinois	
GOODS AND/OR SERVICES AND BASIS INFORMATION		
INTERNATIONAL CLASS	042	
	Providing an internet-based integrated suite	

g fi	format converting; batch data uploading and downloading; search engine and search index generation; pdf generation and support; html file previewing; and mobile/smartphone compatibility.	
FILING BASIS S	SECTION 1(b)	
ATTORNEY INFORMATION		
NAME Jo	John A. Cullis	
ATTORNEY DOCKET NUMBER 1	17699-04T1	
FIRM NAME	Neal Gerber & Eisenberg LLP	
STREET T	Γwo N. LaSalle Street, Suite 1700	
CITY	Chicago	
STATE II	Illinois	
COUNTRY	United States	
ZIP/POSTAL CODE 6	50602	
PHONE 3	3122698000	
FAX 3	3122691747	
EMAIL ADDRESS ip	ipdocket@ngelaw.com	
AUTHORIZED TO COMMUNICATE VIA EMAIL Y	Yes	
OTHER APPOINTED ATTORNEY a	all attorneys at the law firm	
CORRESPONDENCE INFORMATION		
NAME Jo	John A. Cullis	
FIRM NAME	Neal Gerber & Eisenberg LLP	
STREET T	Γwo N. LaSalle Street, Suite 1700	
CITY	Chicago	
STATE	Illinois	
COUNTRY	United States	
ZIP/POSTAL CODE 6	60602	

PHONE	3122698000	
FAX	3122691747	
EMAIL ADDRESS	ipdocket@ngelaw.com	
AUTHORIZED TO COMMUNICATE VIA EMAIL	Yes	
FEE INFORMATION		
NUMBER OF CLASSES	1	
FEE PER CLASS	325	
*TOTAL FEE DUE	325	
*TOTAL FEE PAID	325	
SIGNATURE INFORMATION		
SIGNATURE	/Rakesh Madhava/	
SIGNATORY'S NAME	Rakesh Madhava	
SIGNATORY'S POSITION	President	
DATE SIGNED	01/27/2010	

Trademark/Service Mark Application, Principal Register

Serial Number: 77922469 Filing Date: 01/28/2010

To the Commissioner for Trademarks:

MARK: PRESERVATION CLOUD (Standard Characters, see mark)

The literal element of the mark consists of PRESERVATION CLOUD.

The mark consists of standard characters, without claim to any particular font, style, size, or color.

The applicant, NextPoint Inc., a corporation of Illinois, having an address of

4043 North Ravenswood Ave., Suite 317

Chicago, Illinois 60613

United States

requests registration of the trademark/service mark identified above in the United States Patent and Trademark Office on the Principal Register established by the Act of July 5, 1946 (15 U.S.C. Section 1051 et seq.), as amended, for the following:

International Class 042: Providing an internet-based integrated suite of applications, storage, and grid computing capacity for litigation and trial support services and graphical presentation services that include the following functionality: image generation, viewing and manipulation; text and metadata extraction; batch file format converting; batch data uploading and downloading; search engine and search index generation; pdf generation and support; html file previewing; and mobile/smartphone compatibility. Intent to Use: The applicant has a bona fide intention to use or use through the applicant's related company or licensee the mark in commerce on or in connection with the identified goods and/or services. (15 U.S.C. Section 1051(b)).

The applicant's current Attorney Information:

John A. Cullis and all attorneys at the law firm of Neal Gerber & Eisenberg LLP

Two N. LaSalle Street, Suite 1700

Chicago, Illinois 60602

United States

The attorney docket/reference number is 17699-04T1.

The applicant's current Correspondence Information:

John A. Cullis

Neal Gerber & Eisenberg LLP

Two N. LaSalle Street, Suite 1700

Chicago, Illinois 60602

3122698000(phone)

3122691747(fax)

ipdocket@ngelaw.com (authorized)

A fee payment in the amount of \$325 has been submitted with the application, representing payment for 1 class(es).

Declaration

The undersigned, being hereby warned that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. Section 1001, and that such willful false statements, and the like, may jeopardize the validity of the application or any resulting registration, declares that he/she is properly authorized to execute this application on behalf of the applicant; he/she believes the applicant to be the owner of the trademark/service mark sought to be registered, or, if the application is being filed under 15 U.S.C. Section 1051(b), he/she believes applicant to be entitled to use such mark in commerce; to the best of his/her knowledge and belief no other person, firm, corporation, or association has the right to use the mark in commerce, either in the identical form thereof or in such near resemblance thereto as to be likely, when used on or in connection with the goods/services of such other person, to cause confusion, or to cause mistake, or to deceive; and that all statements made of his/her own knowledge are true; and that all statements made on information and belief are believed to be true.

Signature: /Rakesh Madhava/ Date Signed: 01/27/2010

Signatory's Name: Rakesh Madhava Signatory's Position: President

RAM Sale Number: 770

RAM Accounting Date: 01/29/2010

Serial Number: 77922469

Internet Transmission Date: Thu Jan 28 14:34:51 EST 2010 TEAS Stamp: USPTO/BAS-63.85.229.130-2010012814345106

7688-77922469-46074fa4938ba0d9ea535931f2 367b5a6-DA-770-20100127153946119248

PRESERVATION CLOUD

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE TRADEMARK TRIAL AND APPEAL BOARD

VS. NEXTPOINT, INC.,	Opposer, Applicant.	Mark: PRESERVATION CLOUD Serial No.: 77/922,469 Opposition No. 91198858 Published in the Official Gazette on November 9, 2010		
CERTIFICATE OF SERVICE				
I, Christopher R. Edgar, am over the age of eighteen and not a party to the above-				
referenced action. On October 5, 2012, I served the following document by FedEx				
overnight delivery:				
OPPOSER CASECENTRAL, INC.'S NOTICE OF RELIANCE NO. 1				
I served the foregoing document by FedEx overnight delivery on the counsel listed below:				
Daliah Saper, Esq. Saper Law Offices 505 N. Lasalle, Suite 350 Chicago, IL 60654 Attorneys for Applicant Nextpoint, Inc.				
I declare under penalty of pe	rjury that the foreg	going is true and correct.		

Dated: October 5, 2012

Christopher R. Edgar